NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SYSTEM OF SYSTEMS ENGINEERING AND INTEGRATION PROCESS FOR NETWORK TRANSPORT ASSESSMENT

by

Matthew B. Rambo

September 2016

Thesis Advisor: Warren Vaneman
Co-Advisor: Anthony Russell

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE SYSTEM OF SYSTEMS ENGINEERING AND INTEGRATION PROCESS FOR NETWORK TRANSPORT ASSESSMENT	**5. FUNDING NUMBERS**
6. AUTHOR(S) Matthew B. Rambo	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis proposes a system of systems (SoS) engineering and integration (SoSE&I) process and provides a use case for a network transport analysis that is tailored to an information technology (IT) network. The purpose of the process is to identify the capabilities required for the transport and provide a framework for analysis, test, and implementation to ensure that the network IT system supports the user requirements for the overall SoS. The thesis then details a Navy use case through the steps of the proposed process and provides example steps and criteria for the assessment. Prior research on SoS architectures was leveraged in developing the proposed process and tailored to support IT network challenges.

The thesis makes recommendations to prioritize capabilities, to implement capability-based quality of service (QoS), to have a detailed understanding of applications for the correlation of application to capability, to continuously monitor IT networks to ensure satisfactory performance with new applications or user behavior, and to ensure governance is applied through the process to ensure oversight of design and tradeoff decisions for network throughput analyses.

14. SUBJECT TERMS network transport, SoS architecture, SoS testing, SoSE&I	**15. NUMBER OF PAGES** 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SYSTEM OF SYSTEMS ENGINEERING AND INTEGRATION PROCESS FOR NETWORK TRANSPORT ASSESSMENT

Matthew B. Rambo
Civilian, Department of the Navy
B.S., University of Texas at Austin, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2016

Approved by: Warren Vaneman, PhD
Thesis Advisor

Anthony Russell
Co-Advisor

Ronald Giachetti, PhD
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis proposes a system of systems (SoS) engineering and integration (SoSE&I) process and provides a use case for a network transport analysis that is tailored to an information technology (IT) network. The purpose of the process is to identify the capabilities required for the transport and provide a framework for analysis, test, and implementation to ensure that the network IT system supports the user requirements for the overall SoS. The thesis then details a Navy use case through the steps of the proposed process and provides example steps and criteria for the assessment. Prior research on SoS architectures was leveraged in developing the proposed process and tailored to support IT network challenges.

The thesis makes recommendations to prioritize capabilities, to implement capability-based quality of service (QoS), to have a detailed understanding of applications for the correlation of application to capability, to continuously monitor IT networks to ensure satisfactory performance with new applications or user behavior, and to ensure governance is applied through the process to ensure oversight of design and tradeoff decisions for network throughput analyses.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A&T	acquisition and technology
AAW	anti-air warfare
ADNS	Automated Digital Network System
AEHF	advanced extremely high frequency
AI	Application Integration
ASW	anti-submarine warfare
BMD	ballistic missile defense
C2	command and control
C2P	Command and Control Processor
C4I	command, control, communications, computers, and intelligence
CANES	Consolidated Afloat Networks and Enterprise Services
CBSP	Commercial Broadband Satellite Communications Program
CBWFQ	class based weighted fair queuing
COMSATCOM	commercial satellite communications
COP	common operational picture
CSRR	Common Submarine Radio Room
DOD	Department of Defense
E2C	enterprise, engineering, and certification
EHF	extremely high frequency
FIFO	first in first out
GCCS-M	Global Command and Control System – Maritime
IP	internet protocol
ISP	internet service provider
IT	information technology
LAN	local area network
LoS	line of sight
M&S	modeling and simulation
MILSATCOM	military satellite communications
MWR	morale, welfare, and recreation
NDIA	National Defense Industrial Association

NMT	Navy Multiband Terminal
ODUSD	Office of the Deputy Under Secretary of Defense
PEO	program executive office
PMW	program manager, warfare
PMW/A	program manager, warfare/air
POR	program of record
QoS	quality of service
SATCOM	satellite communications
SE	systems engineering
SHF	super high frequency
SOS	systems of systems
SoSE&I	system of systems engineering and integration
SSE	systems and software engineering
SWaP	size, weight, and power
TCP	transmission control protocol
TDMA	time division multiple access
UDP	unicast datagram protocol
VTC	video teleconferencing
WAN	wide area network
WB	wideband
WGS	wideband global satellite communications
WRR	weighted round robin

EXECUTIVE SUMMARY

This thesis proposes a system of systems (SoS) engineering and integration (SoSE&I) process and provides a use case for a network transport analysis that is tailored to an information technology (IT) network. The following research questions were addressed in the research and development of this process:

1. What are good systems, or SoS, engineering processes to utilize to address network transport design and testing?
2. How can SoS data throughput requirements be identified and assessed to support SoS design and testing activities?
3. What characteristics of supporting tools and simulations are needed to model and characterize network performance as part of the identified systems engineering process?
4. Where should governance be applied to ensure the appropriate decisions are made in terms of identifying the appropriate data rates and QoS policies for the network?

The purpose of the process is to identify the capabilities required for the transport and provide a framework for analysis, test, and implementation to ensure that the network IT system supports the user requirements for the overall SoS. The process is depicted as a circular process as it will be repeated constantly to ensure that any changes to the component systems are supported within the network design. The model is based on leveraging prior SoSE&I research to include the Trapeze model and this proposed model is depicted in Figure 1. The governance and specific steps for network IT systems were added to show the relationship of governance throughout all of the steps (Vaneman and Jaskot 2013) to tailor to an IT system.

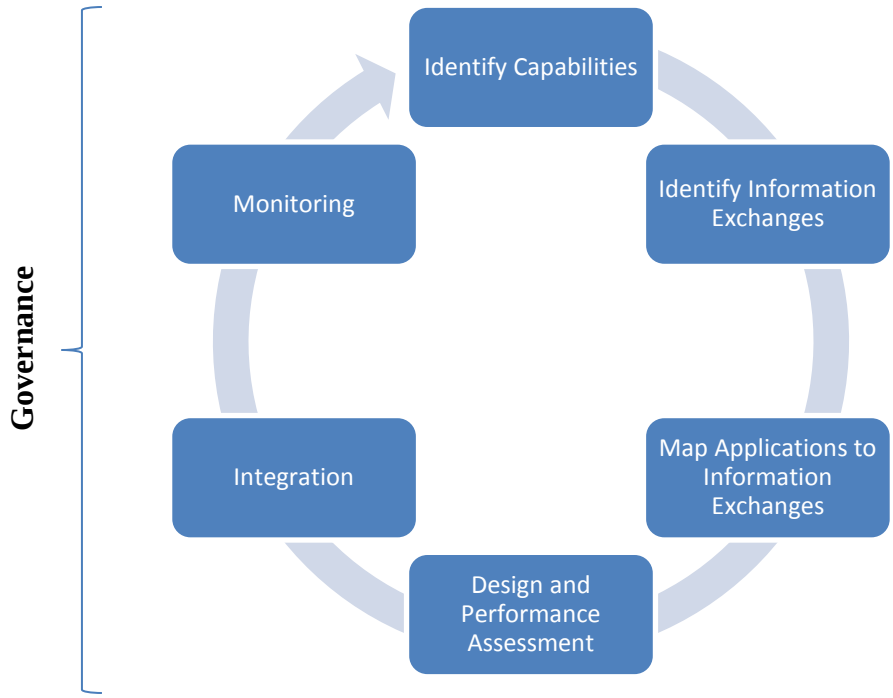

Figure 1. Circular Process Flow for IT Network Design. Adapted from Dahmann et al. (2011).

Once the process is created and detailed, a Navy tactical platform use case is leveraged to run through the proposed process. The implementation with the use case provides the opportunity to assess the steps of the process and development of criteria for the assessment. The Navy scenario is leveraged for the use case to identify and prioritize capabilities, assess information exchanges through the Navy IT system, and provide an assessment of the design to support multiple scenarios with varying data rates available. The use case exercises the process through each of the steps in a Navy platform-representative environment.

Key recommendations from the research and development of the process are to prioritize capabilities and the implementation of capability-based quality of service (QoS), have a detailed understanding of applications for the correlation of application to capability, continuously monitor IT networks to ensure satisfactory performance with new applications or user behavior, and ensure governance is applied through the process to ensure oversight of design and tradeoff decisions for network throughput analyses.

References

Dahmann, Judith, George Rebovich, Ralph Lowry, JoAnn Lane, and Kristen Baldwin. 2011. “An Implementers’ View of Systems Engineering for Systems of Systems.” Accessed August 5, 2016. http://www.acq.osd.mil/se/docs/ImplementerViewSE-SOS-Final.pdf.

Vaneman, Warren, and Roger Jaskot. 2013. “A Criteria-Based Framework for Establishing System of Systems Governance.” *Systems Conference (SysCon)*, 2013 IEEE International, 491–496. doi:10.1109/SysCon.2013.654992.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Professor Warren Vaneman for meeting with me throughout the process of writing and updating this thesis and providing timely feedback on the drafts. His support was invaluable in guiding the research, shaping the scope of the topic, and ensuring that I had access to the latest system of systems materials. His clear expertise in this area was valuable throughout the development of this thesis. Anthony Russell, as co-advisor, also provided many insightful comments to help shape this paper to be clear and concise. I would like to thank the PD21 team of Wally Owen, Kristin Giammarco, Heather Hahn, and Barbara Berlitz. They were exceptional in terms of providing all of the necessary deadlines and resources needed to be successful. They also ensured that the students in the cohort kept their focus on the goal of graduation. Lastly, to my wife, Cathryn Rambo, and my children, Colby and Haley Rambo, thank you for letting me get through the long days and nights of writing this thesis. It would not have been possible without your support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The purpose of this thesis is to identify and detail a systems engineering process to identify requirements and support design and testing for network transport systems that are part of a system of systems (SoS) architecture. This research will add to existing SoS research and network systems with a focus on data throughput analyses. The benefit of this research and the resulting process is to provide an enhancement of IT network design and analysis. This process will ensure accurate information is available to characterize the systems within the SoS architecture during design activities, enhance end-to-end testing with more accurate and measured data, and support validation of engineering models to predict behavior. A secondary benefit is that it can be used to support an early assessment of data exchange requirements for SoS systems to support trade off analyses earlier in the design phase, allowing gaps to be identified earlier to allow more time to address them.

A. BACKGROUND

A SoS is formally defined as "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities" (ODUSD[A&T]SSE 2008, 4). Information technology (IT) network systems and applications fit into this definition due to the interdependency of the systems and integration required to ensure support of information exchanges. Appropriate network services also need to be established to support facilitation of these data exchanges as well as protection of the applications from network threats. Individual applications utilize network transport for support of information exchanges through internet Protocol (IP) transport that allows greater sharing of information and services when the systems are integrated together than if they are standalone systems. Applications rely on the Local Area Network (LAN) to connect users to services local to a site and on the Wide Area Network (WAN) to access services at remote sites for information exchanges outside of the site. The scope of this research will be on network throughput as part of the SoS, but

the other capabilities are critical as well such as cyber protection and other network services within the IT SoS architecture.

A typical LAN and WAN configuration with general functions provided by each system is shown in Figure 1. This diagram was created to depict network functions utilized within IT networks (Miller 2004). All of the applications that require connectivity to remote sites need to traverse through the WAN aggregation points. At the WAN, routing and quality of service prioritization occurs to ensure support of the information exchanges.

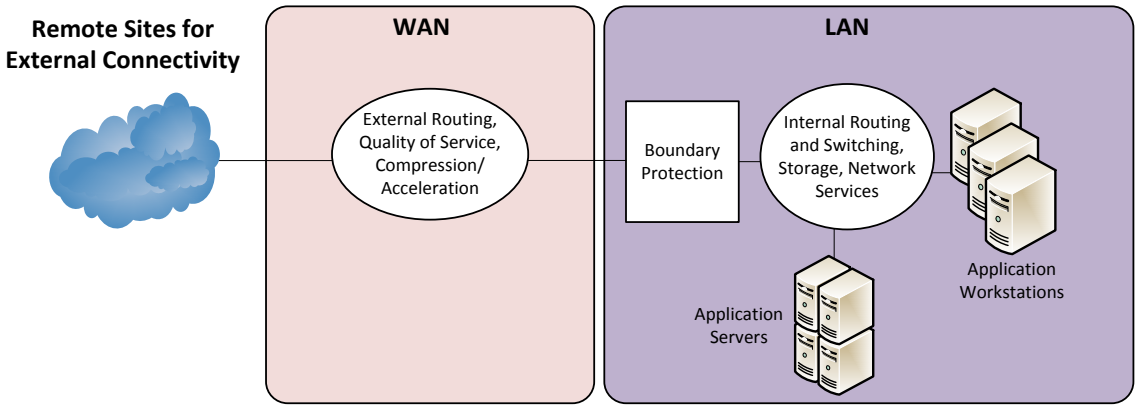

Figure 1. LAN and WAN Diagrams. Adapted from Miller (2004).

From the WAN to remote sites, a bottleneck occurs at the network aggregation points. This is depicted in Figure 2. At this bottleneck, a portion of the network traffic needs to be dropped when the overall data rate at the bottleneck cannot support all of the aggregated network traffic (Miller 2004). There are a number of methods to support the dropping of network traffic when this congestion occurs. This congestion handling should be conducted in a manner that maintains priority traffic even under congestion at the bottleneck points.

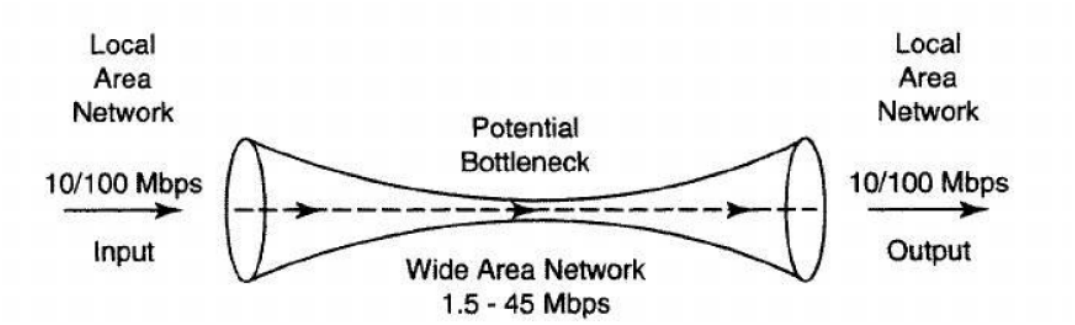

Figure 2. WAN Bottleneck. Source: Miller (2004, 627).

Specific to throughput over network transport, two key factors need to be considered. The first is available bandwidth. This is the raw data rate over the links between the sites and represents the data rates at the smallest point of the bottleneck. This typically needs to be pre-planned and the overall cost increases as this data rate is increased. This could be in the form of paying additional costs to the internet service provider (ISP) such as Time Warner Cable for home or commercial sites. In a standard home or office environment, WAN data rates can be sized to support the information exchanges required in all but the most stressing conditions. However, businesses try to optimize bandwidth to minimize cost. This optimization needs to be performed in a methodical fashion to ensure that data rates can be met in peak conditions to support critical data flows. The nature of what makes those data flows critical depends on the business, consumer, or military user and needs to be well known prior to implementing the network.

The second factor is the quality of service (QoS) policy that determines which information exchanges utilize the available bandwidth when under congestion. The bottleneck remains the same, but the traffic supported through the narrowest point of the bottleneck is controlled by identifying and prioritizing critical traffic types over other traffic. If enough bandwidth is not available, the QoS policy determines the utilization of that limited bandwidth based on network configurations (Park 2005). This is particularly significant for users with limited bandwidth available. Examples of the types of users that fall into this category are consumers in rural areas in the United States, populations in

many non-developed countries, or military users reliant on satellite communications that do not have access to large amounts of bandwidth. These configurations need to ensure identification of the necessary traffic types and prioritization of those traffic types based on the requirements of the SoS architecture. In these cases, it is critical to understand network limitations and ensure prioritization of network traffic to support critical information exchanges. This allows effective utilization of the limited bandwidths available even when peak conditions are not present. To do this, a network designer and administrator need to understand the applications on the network and have a detailed knowledge of the transport requirements of those applications.

B. PROBLEM STATEMENT

There are a number of key challenges associated with IT systems in general for network transport. IT SoS architectures typically contain a large number of interdependent systems to include applications and transport, each site that has an IT SoS is typically unique in terms of user behaviors and actual loaded applications, and the overall number and rate of information exchanges can vary widely based on the mission or activity ongoing. These challenges make it difficult to predict the actual network throughput requirements to meet different scenarios.

The key problem statement to be addressed by this research is as follows: The large number of applications, dependencies, and differences of user behavior for IT network systems make it a challenge to design an IT network SoS architecture to meet the overall requirements and be able to predict the behavior of the SoS architecture in differing conditions.

C. RESEARCH QUESTIONS

Based on the background provided, challenges identified, and problem statement, a system of systems approach is needed to ensure network transport design is being done with the consideration of all the systems that will utilize the network. The thesis will address the following primary research questions in exploring this topic:

1. What are good systems, or SoS, engineering processes to utilize to address network transport design and testing?
2. How can SoS data throughput requirements be identified and assessed to support SoS design and testing activities?
3. What characteristics of supporting tools and simulations are needed to model and characterize network performance as part of the identified systems engineering process?
4. Where should governance be applied to ensure the appropriate decisions are made in terms of identifying the appropriate data rates and QoS policies for the network?

D. OBJECTIVE

The objective of this study is to define an engineering process which ensures that overall network throughput and supporting network design is thoroughly assessed for the necessary information exchanges that need to be supported by the IT network system. This process should be based on existing SoS research and engineering practices. Without having a comprehensive assessment and understanding of how the IT network system will work in a number of different scenarios, the network will not support the required information exchanges when they are needed. This makes the problem statement and resulting research questions critical to address.

E. APPROACH

The approach taken in this study to answer the identified research questions was to conduct a literature review for systems engineering processes relevant to SoS architectures and identify and provide recommendations for modifying these processes to support network throughput analyses. These modified processes will be described to support general IT networks and then be utilized in a sample use case for a Navy network transport architecture to ensure that the processes are supportable. Specific criteria and application to the Navy use case for these processes will be detailed. Lastly, recommended requirements for tool sets to support modeling and simulation as part of the overall systems engineering processes will be detailed to ensure the analysis will provide the necessary information to support the IT network design.

F. SCOPE OF THE STUDY

The focus of the study and use case will be on bandwidth assessments as a consideration for IT networks. However, the key concepts would also apply to other areas such as common network storage, security controls, and general application interoperability that require a complex interdependency with the IT Network service provider and the applications that utilize the network. These other areas are outside of the scope of the detailed study but could be addressed in follow on research. These areas have similar challenges in terms of diverse sets of applications and different usage at each site that make a common approach difficult to manage.

The study also identifies requirements and considerations for modeling and simulation tools to support systems engineering assessments but does not go into detail on generating and assessing network throughput as part of the modeling and simulation activities. This would need to be part of a follow on assessment.

G. ORGANIZATION

This thesis contains the results of a literature review to identify current research on the field of SoS and systems engineering processes in section two. These identified systems engineering processes will be assessed against general network transport architectures and a recommended systems engineering process to address IT networks will be provided in section three. A Navy-specific use case will then be detailed in section four with additional challenges that are more restrictive due to a unique environment, though the concepts from the use case can apply in a broader scope to commercial and consumer applications. These engineering processes will be assessed against this Navy-specific use case to assess the viability of the identified systems engineering process. Lastly, the results of the research and identified process will be provided.

II. LITERATURE REVIEW

A literature review was conducted on SoS design and integration for the key challenge areas identified with IT networks and throughput analyses. Key areas of research are listed in the below sections. The research cited provides details on IT networks and lists the types of SoS architectures, SoSE&I models that are used to depict SE processes, considerations of testing with SoS, and the importance of governance in a SoS construct with multiple stakeholders and an evolving architecture.

A. IT NETWORKS

The *Internet Technologies Handbook: Optimizing the IP Network* (Miller 2004) provides an overview of internet technologies. The range of topics important to this thesis include an overview of network architecture, IP packet delivery, end to end reliability, converged networks covering data and multimedia communications, and network and performance management. This sets the foundation for the underlying network principles that are the subject of the assessment for the network transport in the SoS architecture.

A generic multi-LAN environment depicting multiple LAN's connected by an IP network is provided in Figure 3. The LAN includes the convergence of voice and video capabilities onto the network. The IP network in between sites can be a private connection for greater control of congestion and available data rates or via a leased line shared by other users that may be outside of the control of an organization (Miller 2004). These two primary scenarios impact the level of control and prediction that can be done in assessing network transport. For a private, managed connection between two sites, the parameters of the connection are known and traffic flows understood as the usage of that connection is fully within the control of the organization. For the shared network connection, it is more difficult to predict and model all of the IP traffic on the network as other organizations and users leverage the connection.

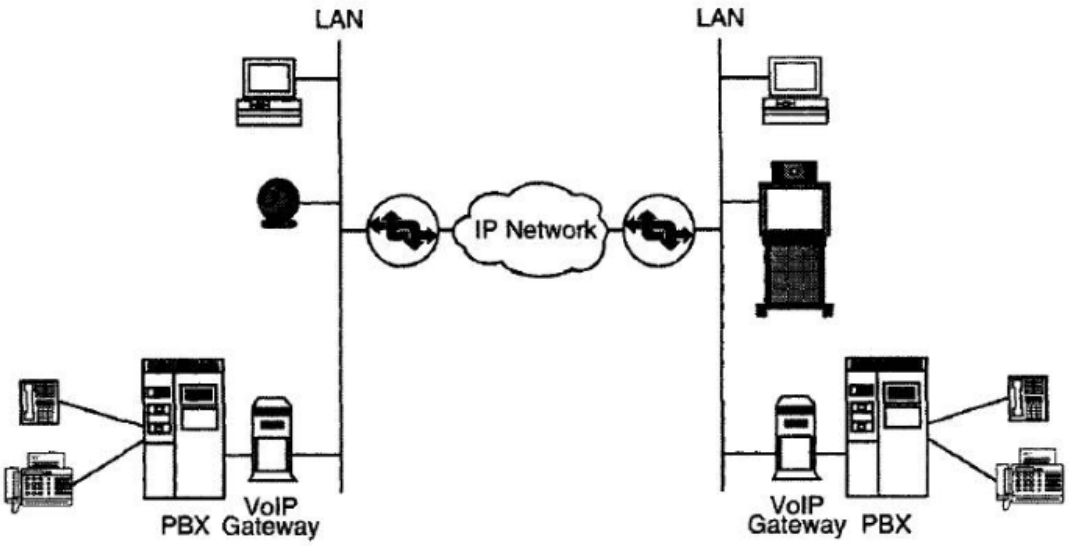

Figure 3. Converged Network Architecture. Source: Miller (2004, 433).

Specific to application data transfers over the network, the Open Systems Interconnect (OSI) layers are critical to understanding the behavior of the IP transport for the various applications. Applications and data flows utilize different abstracted layers within the transport which can impact how they traverse through the network and overall throughput utilization within the network. These layers are captured through the OSI model which is depicted in Figure 4. The connectivity function layers are particularly important to understand and characterize during throughput analyses as this drives the performance of data flows over the network transport. The network layer establishes the path from source to destination and controls congested information packets throughout the subnet. The transport layer is responsible for ensuring end to end reliability of data flows. The transport layer protocol segments longer messages into individual network packets for transmission and reassembles at the receiving node (Miller 2004). Depending on the transport layer protocol utilized, this segmentation, reassembly, and assurance of delivery can vary resulting in a different data flow behavior through the network. The layers all work together to support application data flows over the network. As those layers change, there is potential to impact the behavior of the flow of information through the IT network (Miller 2004).

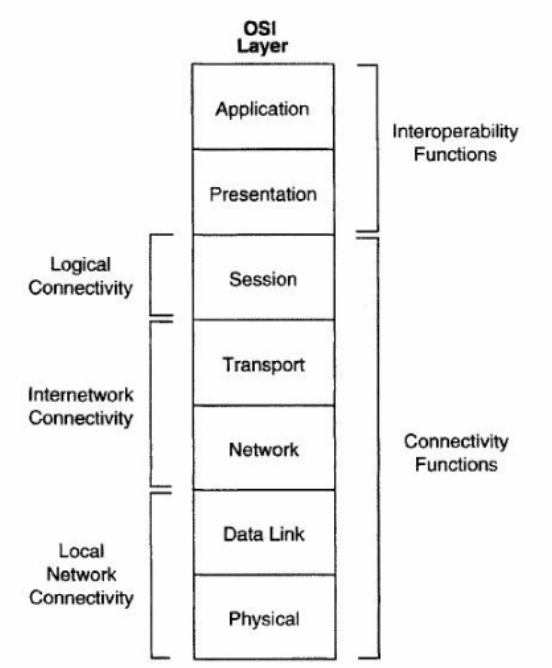

Figure 4. OSI Layer. Source: Miller (2004, 22).

The OSI model is critical to understanding the behavior of applications over the network. As different applications use different protocols, the underlying transport behavior and QoS implementation will vary. During the detailed design and performance assessments of the architecture, the OSI layers need to be understood and modeled to sufficient detail to characterize the behavior of the networks and applications.

B. SYSTEM OF SYSTEMS ENGINEERING AND INTEGRATION

In the IEEE paper "The System of Systems Engineering and Integration 'Vee' Model" (Vaneman 2016), the concept of system of systems is identified and recommendations provided for integration. The paper identifies the following key elements of System of Systems Engineering and Integration (SoSE&I):

- "Definition and control of a managed SoS baseline that directly tracks to delivered capabilities" (Vaneman 2016, 2).
- "An established SoS validation, verification, and certification process to evaluate delivered capabilities in context of mission performance" (Vaneman 2016, 3).

- "A formal method of governance and change control that puts discipline and rigor into investment decisions at the SoS level" (Vaneman 2016, 3).

Within IT Network systems, all of these are key elements that need to be addressed. Due to the complexity, overall number of systems, and rapid change specific to the networking environment specific to transport, these will be expanded upon as part of this research.

The paper also identifies a SoSE&I "Vee" model. The model highlights the SoS requirements, governance, and analysis areas and is shown as Figure 5. The model is a good starting point for a framework to address Network IT system challenges.

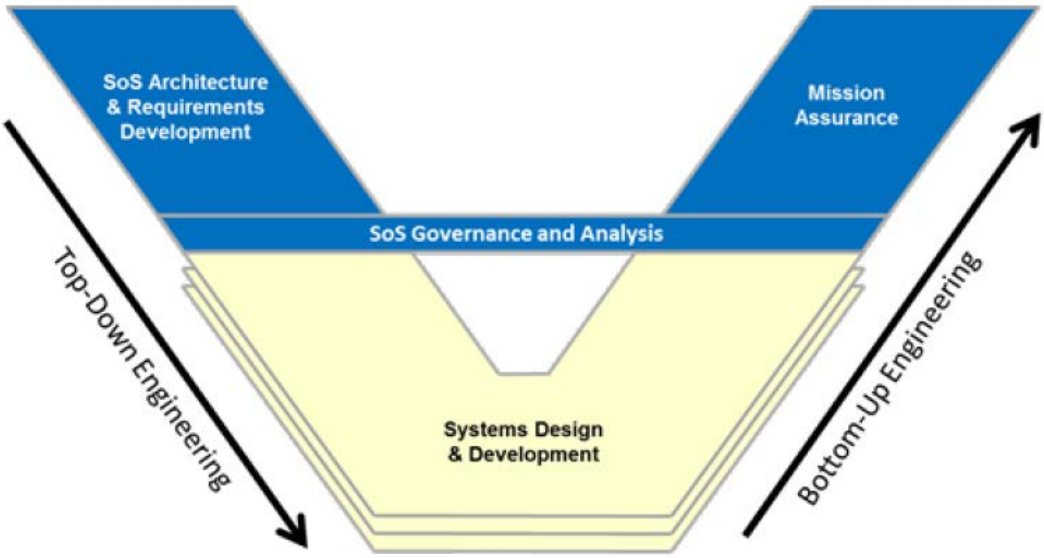

Figure 5. SoSE&I "Vee" diagram. Source: Vaneman (2016, 3).

Vaneman elaborates on SoS activities in the areas of requirements, design and testing. He also stresses the importance of ensuring that the SoSE&I team understands the details of each individual system to ensure compatibility with the entire SoS and for support of the overall mission. These aspects are critical for network transport where a number of interconnecting systems support a number of discrete missions.

C. KEY SOSE&I CONCEPTS

The DOD-sourced "Systems Engineering Guide for Systems of Systems" provides an overview of the SoS environment and SE considerations to support SoS architectures. A SoS is formally defined as "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities" (ODUSD[A&T]SSE 2008).

The four known types of SoS currently are:

- Virtual – "lacks a central management authority and centrally agreed upon purpose" (ODUSD[A&T]SSE 2008, 4).
- Collaborative – "component systems interact more or less voluntarily to fulfill agreed upon central purposes" (ODUSD[A&T]SSE 2008, 5).
- Acknowledged – "recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain independent ownership, objectives, funding, and development and sustainment approaches" (ODUSD[A&T]SSE 2008, 5).
- Directed – "integrated system-of-systems is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose" (ODUSD[A&T]SSE 2008, 5).

Commercial IT systems can vary between the known SoS types depending on how the company and IT system is structured. Larger companies would generally fund their own IT department to provide network transport and services. With common funding and oversight, upgrades would be managed within that group and prioritization of funding and tasking would be driven from the company. The Navy platform IT systems follow most closely an acknowledged system of systems with the tactical networks LAN and WAN providing network services. The applications are typically individual Programs of Record (PORs) that have independent funding lines and schedules. The applications need to work with the LAN and WAN to ensure appropriate integration testing and fielding alignment for installations. Each application owner has a

desire to ensure their own successful integration into the network, but this is not necessarily consistent with the goals of the larger SoS architecture.

Seven core elements of SoSE&I have been identified for usage as a guide in application of systems engineering processes. They are listed verbatim below as defined in the DOD SE guide (ODUSD[A&T]SSE 2008).

- Translating capability objectives
- Understanding systems and relationships
- Assessing performance to capability objectives
- Developing and evolving an SoS architecture
- Monitoring and assessing changes
- Addressing requirements and solution options
- Orchestrating upgrades to SoS

To support the core elements, the authors identify the importance of modeling and simulation (M&S) to support analysis of the SoS architectures and understand the complex interactions of each of the component systems. The authors also stress the importance of identifying the capabilities that the SoS is expected to provide, then use those capability requirements to ensure proper system design and a full understanding of the system interrelationships to meet those capability requirements. It is critical that SoSE&I addresses the end-to-end behavior of the systems to address the key issues that affect that behavior (ODUSD[A&T]SSE 2008).

These core elements are critical to IT network SoS architectures. These will be addressed in the proposed systems engineering processes to ensure that each element is considered during the design, integration, and fielding of the SoS architectures. Within IT network SoS architectures, the core elements of understanding systems and relationships, assessing performance to capability objectives, and addressing the requirements are difficult elements to meet based on the complexity, rate of change, and lack of clear SoS requirements.

D. SOS MODELS

"An Implementer's View of Systems Engineering for Systems of Systems" (Dahmann et al. 2011) contains models that represent the core elements of SoSE&I and interrelationships for SoS capability evolution. The authors describe the Trapeze model to show the various SoSE&I activities that are needed and the linkages throughout the process. The authors then manipulate the Trapeze model to a Wave model to show the SoSE&I activities in a time sequential manner that clearly depicts the iterative approach required through SoS architecture development (Dahmann et al. 2011).

The Trapeze model is shown in Figure 6. This shows the iterative process of SoSE&I that needs to be followed and the relationship with the external environment (Dahmann et al. 2011). As identified in the process, there is a lot of iterative, evolving design and requirements assessment for complex SoS architectures. A detailed understanding of the system is needed and continues to be refined through the SoSE&I process.

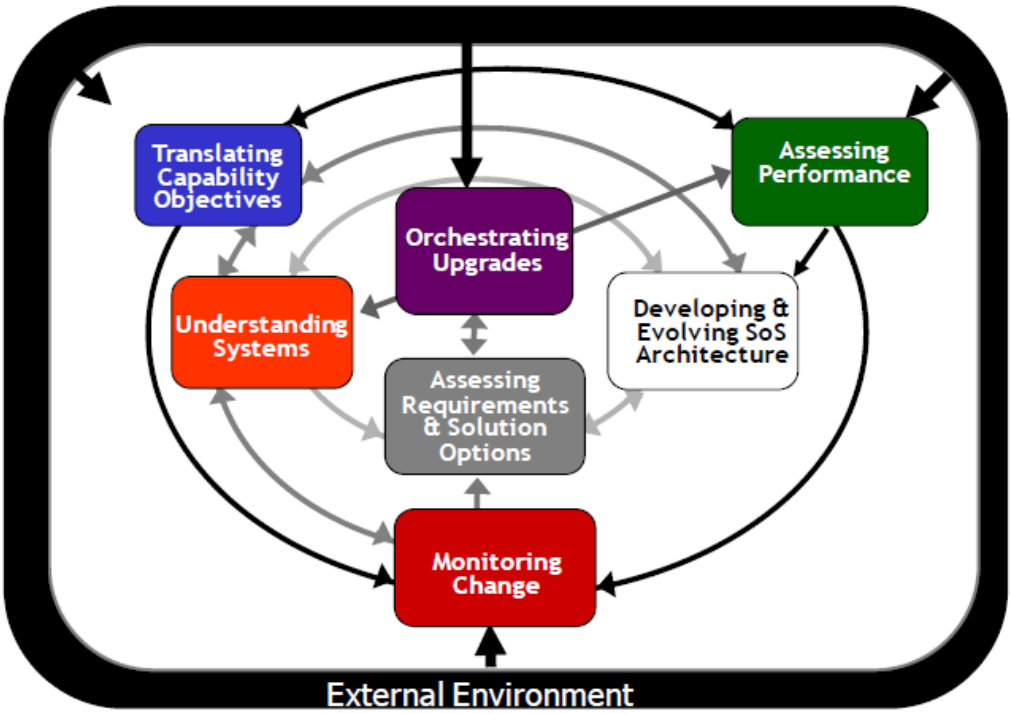

Figure 6. Trapeze Model Depiction of SoSE&I. Source: Dahmann et al. (2011).

Specific to network IT systems, the SoS analysis portion is critical to ensure that the appropriate architectural design decisions are made based on the systems within the architecture. Once developed and planned, the SoS architecture will need to be implemented and monitored with results fed back to the analysis as an evolving architecture. For network systems, this iterative model should be tailored to address the unique aspects of IT network design and be used to support the overarching SoSE&I. This will need to be run frequently and with parallel architectures to ensure the different variations of the architecture are addressed. The trapeze model appears to fit well into analysis and design for network IT SoS architectures, and this has been used as a starting point to identify additional efficiencies to address the specific challenges faced with network systems. The iterative approach of the model is well suited to the dynamic nature of applications and integration into networks due to the number of changes that need to be assessed over time.

E. SOS TESTING

"Systems of Systems Test and Evaluation Challenges" (Dahmann et al. 2010) identifies the challenges of testing for SoS architectures. The authors identify the challenges of verifying performance and behavior of SoS due to increased subjectivity of behavior as well as the number of different systems involved with SoS. The authors also cite complexity of testing due to the overall number of interfaces and systems, causing the need to have a number of different collection points during testing (Dahmann et al. 2010). There are challenges in establishing SoS requirements to test to, as well as ensuring all the component systems are present during test periods to ensure proper interoperability. The authors also identify typical approaches that SoS use to ensure component systems are tested together even when they are not programmatically aligned. Examples include scheduling SoS development into blocks with discrete test events for each. Lastly, the authors identify the importance of assessing performance post-implementation. A way to do that is to ensure proper instrumentation on the systems to monitor their performance once deployed (Dahmann et al. 2010).

These test challenges and approaches identified for SoS are very relevant to network IT systems, in particular for bandwidth assessments. Due to the number of aggregate systems and number of different capabilities that need to be supported through a transport aggregation, the behavior of the systems and type of systems connected to each network need to be understood to be able to characterize the performance.

F. GOVERNANCE

"A Criteria-Based Framework for Establishing System of Systems Governance" (Vaneman and Jaskot 2013) addresses the governance for the SoS architectures: "Governance is the set of rules, policies, and decision-making criteria that will guide the SoS to achieving its goals and objectives" (1).

Network transport systems require governance through the design and analysis phases of the SoSE&I. The rules, policies, and decision-making criteria should be clearly defined to ensure that the design and integration activities are focused with clear direction for the overall SoS. For limited transport systems, there need to be tradeoffs between missions and applications for transport out of each site. These tradeoffs need to be managed to ensure support for the most critical applications and corresponding missions. A governance process is key to ensure that decisions are being made during the design and integration process to ensure the right tradeoffs are being made. Each individual user of the network is going to feel that their tasking is important, but governance allows a more holistic assessment of the entire system of systems architecture to ensure that the right priorities are being addressed. For commercial IT systems, governance is conducted by the company management. In the case of Navy IT systems, governance should be conducted by the technical authority with appropriate warfighter input.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

Based on the literature review conducted for IT networks and SoS, previous research can be leveraged to define a tailored SoS engineering process to capture appropriate design, testing, and implementation steps throughout the life cycle of the IT network system. This section identifies the core components of general IT networks, discusses the specific challenges associated with IT networks that need to be addressed with a SoS approach, and details the tailored process that was created leveraging the research on SoS.

A. GENERAL IT NETWORK OVERVIEW

A network IT system comprises network devices, servers, and workstations that integrate into a larger SoS to allow the utilization of network transport for support of information exchanges through internet Protocol (IP) transport that allows greater sharing of information and services when the systems are integrated together. Applications rely on the LAN to connect users and servers' local to a site and on the WAN to access remote sites for information exchanges outside of the site. As discussed in the introduction, this research focuses on network throughput design and assessment and the two key areas—data rate and QoS for WAN transport. To support ensuring that the data rates are appropriately sized, the behavior of the network and underlying applications and information exchanges need to be understood. At points of congestion, the QoS ensures that the bandwidth is utilized in an effective manner. This is crucial as part of the network design to ensure that the SoS architecture is meeting the needs of the users.

B. DETAILED CHALLENGES

There are a number of key challenges associated with IT systems for network transport. These challenges make it critical to have a well-defined process for capturing information exchange requirements and ensuring that the transport is suited to support these requirements. With the rate of change and number of factors that need to be taken into account, this process will need to be flexible and repeatable. If these challenges are

not addressed, the IT network will not support the capabilities required by the users when needed and the design of the SoS architecture will not fully meet end user requirements.

The first challenge is the complexity of trying to model and predict the behavior of the architecture due to the number of interdependent systems that make up the overall SoS network transport for a site. This includes routers, switches, applications, servers, and typically security components such as a firewall for network protection. These systems need to interoperate together to ensure network transport is provided. If this SoS cannot be understood, it will not function as intended and not meet user requirements for data transport. Applications connect to the LAN via a switching infrastructure. This supports internal site connectivity as well as being part of the path for transport to remote sites. The LAN then connects to the WAN and required security devices. The WAN component then utilizes remote connections to reach other users outside of the local network. The applications have logical interfacing with all the components in transport even though they are physically connected to the LAN. The network security components need to be configured to allow data flows while still maintaining appropriate network protection for the IT systems. The WAN devices need to support routing based on the destination and prioritization of critical applications over non-critical applications within the congestion points of the network. The remote connections need to be set up to support the necessary bandwidth to ensure that, even with prioritization, enough data can be transmitted (Miller 2004). In a standard commercial environment, these systems are all typically designed and implemented by the company IT department as a directed SoS architecture. The company resources the various components and ensures that the resources are applied in a priority aligned with the company goals.

The second challenge is the number of variances with network transport between each site, making it difficult to have a common design for each of the sites. The result is increased design and testing activities due to the variances and increased configuration management complexity to maintain a number of different configurations. Two remote branches of a business may have equivalent hardware and software, but a varying amount of users and mixture of different applications based on the focus of the site can greatly change the requirements for bandwidth on network transport. An engineering team may

utilize more bandwidth for distributed software simulations. A different site with a public-facing website may experience more users connecting to it than a less busy site, which could modify the transport requirements. These variables make it challenging to have a common configuration amongst different sites.

Lastly, it is difficult to predict the overall number of information exchanges and aggregate data rates needed for remote connections. Each user varies in the type and operations of applications. Some users may be more active in the morning, whereas others may be productive in the afternoon, leading to an increased utilization of network transport at those peak times. Depending on the type of business, the network transport will be stressed at different times due to different reasons. A stock market company will be very active when there are large changes in stock market pricing on a given day. A humanitarian organization will be more active when a natural disaster occurs.

Changes in the applications themselves can also change the demands on network transport. A software patch migrating to encrypted data transfers can increase the utilization over the network to account for encryption overhead, even if the end users have no change to their tasking or behaviors. A change to a website can increase the demand for information exchanges by including an embedded video that plays when users access the site. These changes are not typically planned and cannot be controlled well for outside hosted websites but need to be accounted for in sizing the transport. Each of the large number of systems has a number of interfaces with other systems, for a large number of different traffic flows. Additionally, these information exchanges support a number of different areas ranging from lower criticality such as Facebook web browsing, to important but not time sensitive such as ordering replacement supplies, to time critical for support of a critical task such as ensuring the stock order is placed. Having an understanding of these data flows and how they are utilized is critical to understand the sizing of the network. All of these considerations need to be taken into account when designing and testing the network transport.

C. PROCESS

The following sections detail the methodology to support the network transport assessment. This is intended to address the challenges identified and ensure appropriate design and testing activities for an IT network. The general recommended process flow is depicted in Figure 7. The key steps of the process include identifying the capabilities, identifying information exchanges, mapping applications to the information exchanges, designing the network transport and assessing performance, integrating the design, ensuring governance of any design tradeoffs, and monitoring of the installed network to identify any changes in network behavior that would require a re-assessment to the design. This is depicted as a circular process as it will be repeated constantly to ensure that any changes to the component systems are supported within the network design. This model is based on the Trapeze model that was previously introduced SE (Dahmann et al. 2011). The key concept of an iterative approach and many of the common steps of the model was captured, but governance and specific steps for network IT systems were added to show the relationship of governance throughout all of the steps (Vaneman and Jaskot 2013) and to tailor to an IT system.

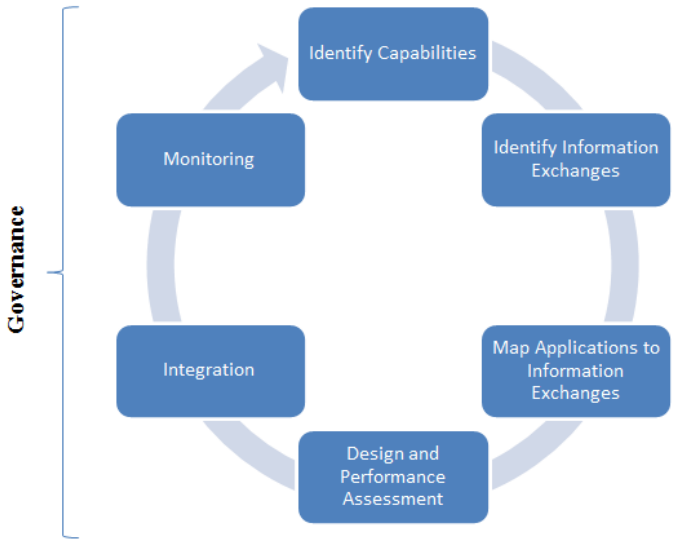

Figure 7. Circular Process Flow for IT Network Design. Adapted from Dahmann et al. (2011).

A different view of the process and corresponding steps and the key questions to be addressed at each step of the process is provided in Figure 8. This provides more detail of the specific focus areas of each step. These steps are individually detailed further in this section as well.

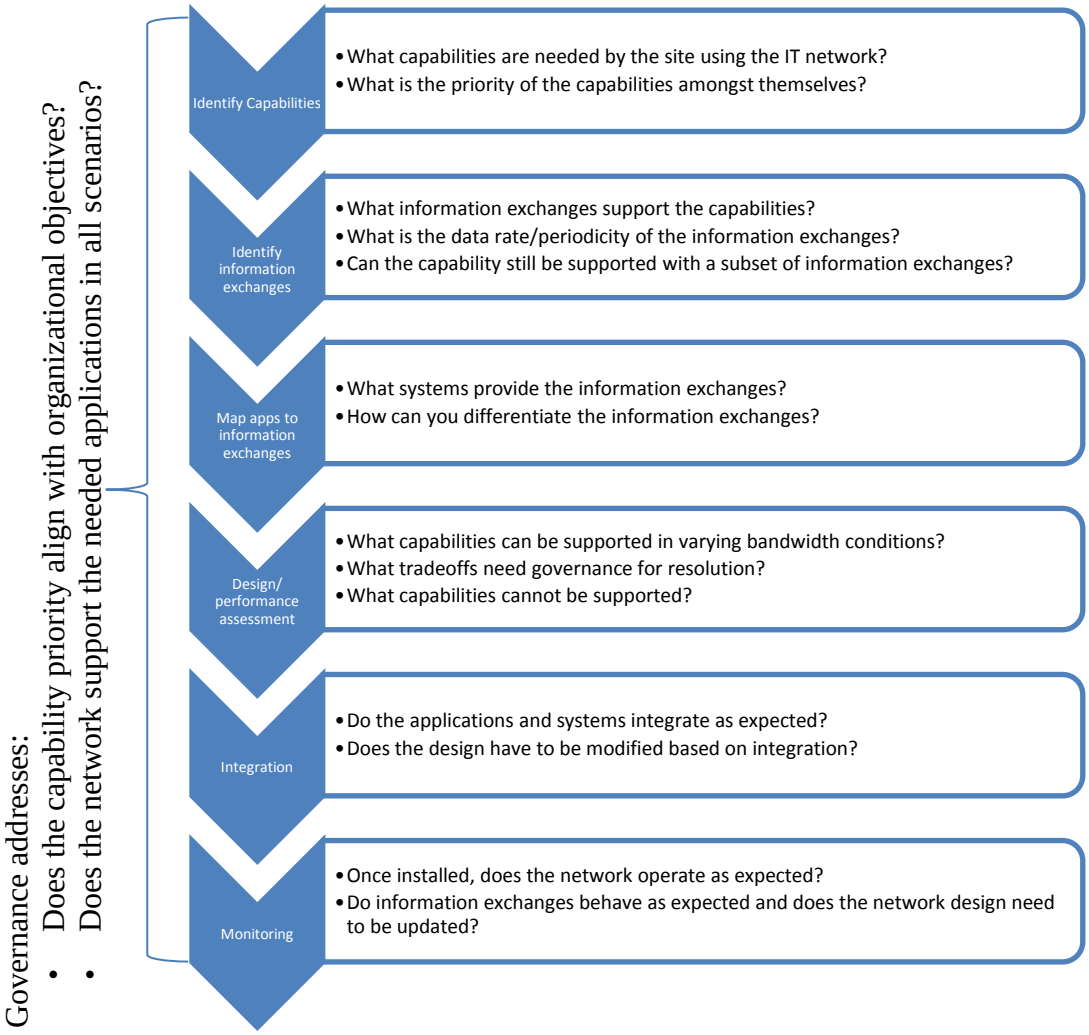

Figure 8. Detailed Process Flow.

1. Identify Capabilities

The capabilities that the network needs to support are critical to identify. A depiction of typical capabilities required for an IT network for a commercial company is provided in Table 1. The capabilities vary based on the type of company but the general

categories would be similar. The key is to identify the known capabilities and prioritize them to support analysis of the design of the network transport. Three categories of high, medium, and low are depicted here but more categories could be identified as needed for more granular assessments. By categorizing the capability by priority, tradeoff decisions can be better informed during the design and analysis phases. This step is often missed when designing a network IT architecture, but is important to ensure that the focus is provided to the critical applications to any network. By ensuring tracking of all the applications that support a critical capability, those applications can then be prioritized over lower priority applications when congestion occurs.

As capabilities are added, they need to be considered as part of the network design. This step should be repeated as new capabilities are identified that are reliant on the network for operations.

Table 1. Capabilities and Prioritization. Adapted from Miller (2004).

Capability	Priority (High/Med/ Low)	Description
Critical Business Traffic	High	Network traffic critical to the business (financial, customer exchanges)
Logistics	Medium	Network traffic for maintenance of equipment
Non-time sensitive Business traffic	Medium	Network traffic in support of the business that is not time critical (online training, general email)
Employee Leisure	Low	Non-critical network traffic in support of employee leisure (web browsing, personal email)

2. Identify Information Exchanges

Once the capabilities that the network needs to support are identified, the information exchanges to support those capabilities need to be identified. There are typically a large number of information exchanges that need to be supported for each

capability and it is difficult to fully document all of them. This documentation also is typically not maintained even when initially captured, but a full listing and understanding of information exchanges is important to be able to fully characterize the performance of the network.

A depiction of the type of information required for information exchange requirements to be able to assess them for network throughput based on the earlier examples of capabilities for a typical business is provided in Table 2. The information exchange is general in nature and will be tied to a specific application in the next step. All of the information exchanges to support a higher priority capability would be considered very critical in this model.

Table 2. Information Exchanges per Capability. Adapted from Miller (2004).

Capability	Priority (High/ Med/Low)	Information Exchanges
Critical Business Traffic	High	Critical web, critical file transfers, critical voice
Logistics	Medium	Non-critical web, non-critical email, non-critical file transfers
Non-time sensitive Business traffic	Medium	Non-critical web, non-critical email, non-critical file transfers
Employee Leisure	Low	Personal web, personal email

3. Map Applications to Information Exchanges

Once the information exchanges are identified, the next step is to map the applications to those information exchanges. The application is the system or systems that participate in the information exchange. A table that adds to the previous example by adding the appropriate applications for each information exchange is provided in Table 3.

Only the first two capabilities were assessed, but all the capabilities would need to have the appropriate application identified for each exchange based on common applications (Miller 2004).

Table 3. Information Exchange Mapping to Applications. Adapted from Miller (2004).

Capability	Priority (High/ Med/Low)	Information Exchanges	Applications
Critical Business Traffic	High	Critical web	Workstation to company web server
		Critical File Transfers	Workstation to company file transfer server
		Voice Calls	Voice over IP handsets to call manager
Logistics	Medium	Company web	Workstation to company web server
		External web	Workstation to external web server
		Company Email	Workstation to company email server
		File Transfers	Workstation to external file transfer server

For each of the applications and information exchanges, more detailed information is needed to be able to characterize the behavior of the data flow on the network. Specifically, the transport characteristics, data rate, and frequency of the data flows are required. This information should be collected and maintained for each information exchange and corresponding application as part of the overall process.

The transport characteristics of the data flow are needed to be able to characterize the data flow as part of the network design. This includes the source and destination

hosts, the protocol utilized for the data flow, and the port number of the traffic. Standard protocols utilized include Unicast Datagram Protocol (UDP) and Transmission Control Protocol (TCP) (Miller 2004). This information is needed to ensure that critical applications are prioritized within the transport. Additionally, different protocols operate differently under congestion and this should be a factor in the network assessment. For example, TCP will reduce its window size and send less overall traffic under congestion and loss. UDP will send a continuous stream of traffic and will not exhibit the same behavior (Miller 2004). These impact the assessment for network performance and are a factor of sizing and understanding network transport behavior.

The data rate is needed in the analysis phase to be able to understand the data rate variances. By understanding peak, average, and minimum, a traffic flow analysis can be conducted to determine what the peak and standard loads are on the network. Though the peak rate will not always be used, different scenarios should be assessed to determine what conditions are supported. For very critical capabilities, the peak rates of all the supporting applications may need to be supported as a worst case. For less critical capabilities, this may not be worth the cost for the resulting bandwidth to support all peak cases.

The periodicity of the data flows is needed to understand the patterns of the application for data rates. Some flows are continuous whereas others are time-sensitive. The overall traffic flow pattern needs to be understood to determine how the different data flows interact with each other over the network transport. Dependencies of traffic flows amongst each other are also critical to understand. If multiple data flows have peak flows at the same time, this would be a consideration for aggregation of flows as part of the network analysis.

Each parameter and a description that is needed for each data flow are shown in Table 4.

Table 4. Data Flow Parameters and Descriptions. Adapted from Miller (2004).

Parameter	Description
Transport Characteristics	What are the characteristics of the data flow for identification as part of the network design?
-Source System	What system originates the information exchange?
-Destination System	What system receives the information exchange?
-Protocol	What protocol does the application use to support the information exchange?
-Port	What is the TCP/UDP port of the traffic?
Data Rate	Characterize the bandwidth requirements for an information exchange
-Peak Data Rate	Highest data rate that needs to be supported
-Average Data Rate	Average data rate
-Minimum Data Rate	Lowest data rate for the information exchange
Frequency	How often and how long is the information exchange required for each capability?
-Periodicity	How often does the information exchange occur?
-Duration	How long does the information exchange remain once triggered?
-Dependencies	Is the information exchange dependent on a different information exchange concurrently?

4. Design and Performance Assessment

With a clear set of capabilities, information exchange requirements, and applications mapped to those requirements, the design of the IT network system and assessment needs to be conducted. As part of this network analysis, the network transport requirements will be used to identify an appropriate network transport configuration to support the identified requirements. This assessment includes aggregating the overall information exchange requirements for each capability and comparing them against the available bandwidths for the transport in specific scenarios. This step of the process would leverage modeling and simulation to quickly assess a large number of data flows,

scenarios, and data rates to ensure an optimal architecture is selected. These key factors need to be taken into account as part of the design and performance analysis as depicted in Figure 9.

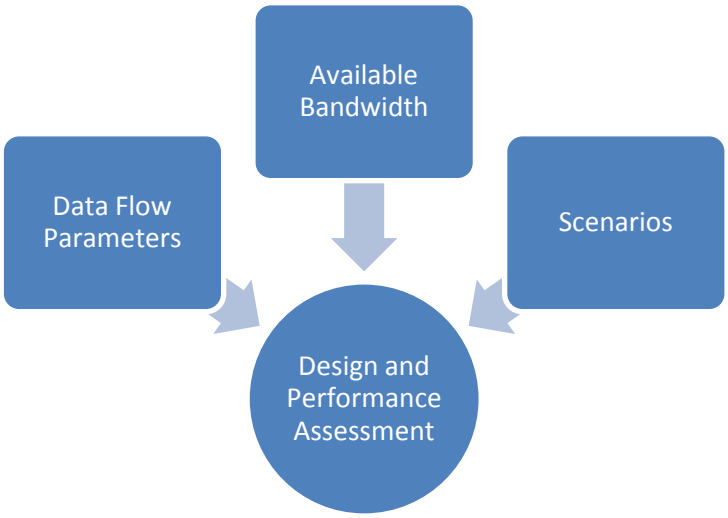

Figure 9. Design and Performance Analysis Factors.

The data flow parameters are taken from the information exchange and application requirements for each capability. The aggregation of data flow rates for each capability should be assessed to determine what bandwidth is needed to support the capability. A probabilistic approach could be used based on the identified data flow parameters to determine the confidence that the data rate would support the data flows associated with that capability. This will be further explored during the use case in the next section. There are going to be cases where one application supports multiple capabilities and is indistinguishable at the congestion points. In these cases, information exchanges for that application should apply to the most critical capability to ensure that it is supported. If a single server is supporting high and low priority capabilities, it is difficult to differentiate data flows supporting the higher priority capabilities from the lower priority capabilities if the same ports and protocols and source and destination IP addresses are being used. Unless a technical implementation drives a distinguishable difference, all data flows for that application will need to be assessed for the higher

priority capability for QoS prioritization under congestion so that the application data flows are supported.

The bandwidth available for connectivity should be included as an input to the performance assessment of network throughput. This could be a combination of links if available for an overall bandwidth. This bandwidth typically would need to be assessed only at congestion points. An office LAN would not likely reach capacity internal to the site with Ethernet connections throughout, but would likely have a congestion point via the WAN connection to remote offices via the internet Service Provider at the WAN bottleneck (Miller 2004). This congestion point would be the focus of the bandwidth assessment to ensure that the rates will meet the capability requirements for the architecture.

Different scenarios should be assessed to support the design. These should account for different bandwidth conditions, such as if one of two links providing transport fails and a limited bandwidth scenario should be assessed. This may drive the need to migrate to an expanded data rate connection if a single link is not adequate. This should also take into account data flow linkages for different capabilities and ensure that the right dependencies are considered. For example, if an urgent situation occurs and a critical capability is needed, it would not be likely that users would be browsing personal email if the business if being impacted so bandwidth would not need to be provisioned to account for personal web browsing in this scenario. These types of scenarios should be considered as part of the overall analysis effort. The scenarios will be specific to the network IT implementation being assessed and should be included in the design and performance analysis to ensure the primary scenarios are considered.

A key area of the assessment is the quality of service (QoS) applied within the network. This dictates how the network devices handle congestion. Many types of QoS methods are possible for queuing of messages (Miller 2004). This should be looked at as part of the design activity. The optimal design would be to have capability-based queuing, where higher priority capabilities would be transmitted first. After higher priority capabilities are met, lower priority capabilities would then be provided the remaining bandwidth. This allows a clear prioritization scheme to ensure that the higher

priority data flows supporting the higher priority capabilities are serviced first over the network. This implementation would be assessed as part of the design and corresponding performance analysis. The QoS is critical to ensuring that the behavior of the network IT architecture is understood and is an important factor in the analysis of a network IT design.

5. Integration

Once the design and performance analysis has been completed, the SoS architecture should be integrated and tested to ensure proper design and analysis (Dahmann et al. 2010). In this integration testing of the architecture, the selected design for the architecture will be validated to ensure it can meet the network transport requirements. This step of the process is where the design team would move from modeling and simulation to a lab or site integration event using the results of the previous modeling and simulation analysis. As initial requirements for the data flows are estimates, the data flow exchange requirements will need to be updated based on measured data rates through integration testing and network analysis as an iterative process. This needs to be repeated until the optimal configuration has been established to support the SoS capability requirements. If the data flow requirements significantly differ from the prior analysis, the design may need to be updated at the previous step with additional modeling and simulation and then come back to the integration step once the design has been updated.

There are several key aspects of integration to consider in this step of the process. The integration team should ensure that user behavior is emulated sufficiently to capture data rates of the various data flows. The systems should be representative of the systems that will be implemented at the site. Some of the scenarios should be assessed to validate expected behavior, though all may not be possible due to time and cost. Lastly, monitoring points should be present for the collection of information on data rate exchanges to validate the information exchange requirements identified during the earlier steps of the process (Dahmann et al. 2010).

6. Governance

In many network IT systems of systems, the bandwidth will not meet capability data flow requirements in all scenarios. This then becomes a decision on tradeoffs of expanding bandwidth with additional cost or accepting the limitations of the architecture based on the selected design. The governance of those decisions is critical to ensure that the limitations of the selected architecture are known, that the right decision makers are aware of the limitations and agree with the tradeoffs, and that the selected design is suitable for implementation. Governance is critical to ensure that appropriate oversight is in place to ensure that the capabilities are prioritized correctly in support of the business and that the design supports that prioritization level. It is needed throughout the process to ensure that the design and integration activities support the overall company objectives (Vaneman and Jaskot 2013). Design decisions by the engineers creating and verifying the design have the ability to make critical decisions that will impact the performance of the network to support the company. Governance ensures that these decisions are made with the appropriate oversight and focus on overall company goals (Vaneman and Jaskot 2013).

To illustrate the need for governance with a trade-off decision, an example is provided here. If a performance assessment was completed with ensuing integration and the bandwidth was determined to not fully support all capabilities, this would need to be identified as a deficiency for the capabilities that are not supported for the SoS architecture as shown in Table 5. In the table, green depicts capabilities that would be supported in all scenarios and yellow depicts capabilities that are degraded at peak times of activity. As shown, all capabilities would not be supported at all times and the lower priority capabilities would not be supported fully. The governance process would need to determine if this is acceptable to the company and, if not, additional bandwidth would need to be identified as part of the IT network design. By identifying and correlating the capabilities to the applications and bandwidth, the appropriate governance decisions can be made based on the capability to ensure that the correct tradeoffs are understood and can be made by the governance process. When a specific application or information

exchange is not supported, without understanding the capability loss an appropriate decision cannot be made.

Table 5. Performance Assessment Mapped to Capability Prioritization.

Capability	Priority (High/Med/ Low)	Description
Critical Business Traffic	High	Network traffic critical to the business (financial, customer exchanges)
Logistics	Medium	Network traffic for maintenance of equipment
Non-time sensitive Business traffic	Medium	Network traffic in support of the business that is not time critical (online training, general email)
Employee Leisure	Low	Non-critical network traffic in support of employee leisure (web browsing, personal email)

7. Monitoring

Once the IT Network SoS is tested, design finalized, and approved via the governance process, it will be implemented operationally. As the simulation and lab environment is different than the production environment, the network transport requirements will need to be further refined with the operational values identified based on user behaviors and changes to applications that connect to the network. These changes should feed back to the requirements and are used to support future updates of the fielded design. Network IT systems need to be continually monitored to assess changes in data rates or flows and ensure that data flow requirements are updated accordingly (Dahmann et al. 2010). If the network IT system is deemed to not meet the capability requirements any longer, the design and analysis step needs to be re-entered to ensure that the network IT architecture meets overall capability requirements.

A number of network monitoring tools are available to identify data flows and ensure monitoring of the bandwidth constrained interfaces. This should be continually

done, with alerts set up to trigger if a threshold has been exceeded where the network IT architecture is no longer meeting data rate requirements for the site (Miller 2004). There are a number of network monitoring tools available to support collection of this information, but proposing specific tools are outside the scope of this research.

D. DETAILED PROCESS

A depiction of each of the steps of the proposed process with linkages for design, integration, and governance is provided in Figure 10. As noted, this process is iterative as it needs to be continually followed, but it also needs to feed back to previous steps if any updates need to be made in the design or collection of information exchanges for each of the capabilities and corresponding applications. The key outputs of the process are listed in the diagram. After the first step, identify capabilities and map to priority, a set of capabilities will be identified and the corresponding priorities of those capabilities. The second step will output a list of information exchanges. The third step will then list the applications and detailed information exchange parameters. After the design and performance assessment, a candidate design will be proposed to enter integration. After integration, a tested design will be available with any identified deficiencies. The governance step will assess the tested design and any limitations, and provide feedback to drive an updated design if needed. If not, a validated design will be provided for implementation and monitoring. With the monitoring step, any updates will need to be identified for the information exchanges to update the design. Lastly, if any new capabilities or changes to existing capabilities are identified, the process will need to be followed for each step.

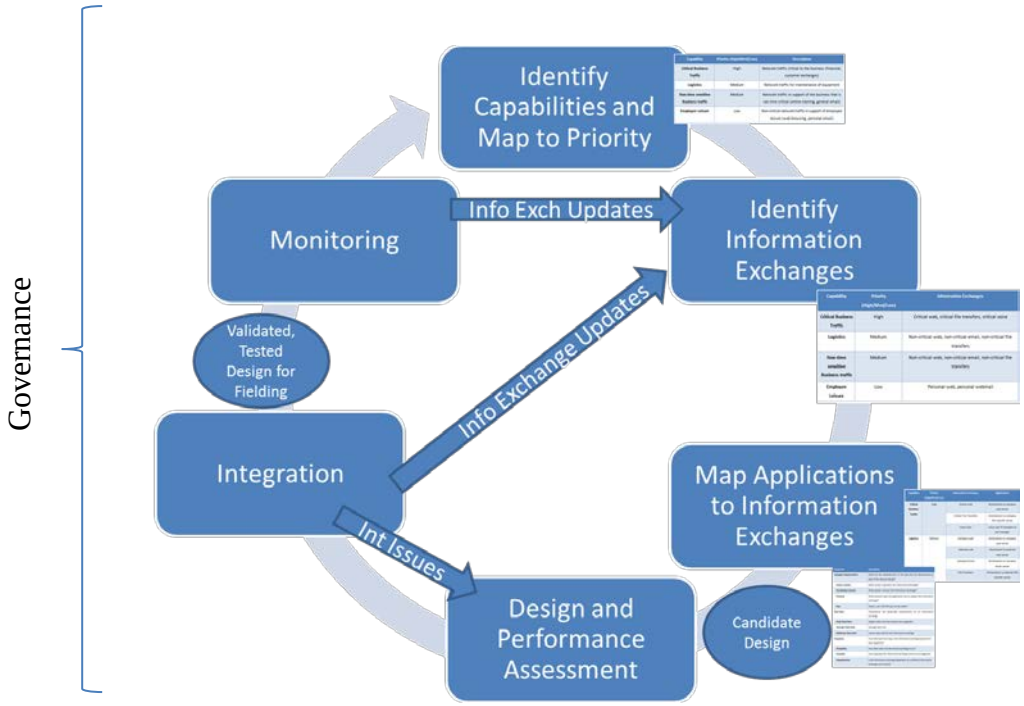

Figure 10. Detailed Process with Outputs and Linkages. Adapted from Dahmann et al. (2011).

This identified process addresses the challenges identified for the Network IT SoS architecture. The following section will take this proposed process and apply to a Navy-specific use case for tactical networks on platforms. Many of the challenges within IT networks apply to tactical networks, but additional challenges apply as well. By stressing the process in a challenging environment, this will ensure the process is executable for many different cases in support of IT network design and implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NAVY INFORMATION TECHNOLOGY USE CASE

The previous section identified a tailored SoSE&I process for usage within IT networks. This process will now be applied to a sample use case for a Navy network transport architecture to ensure that the process is supportable. Navy IT networks have additional challenges that need to be considered and is a stressing use case for the proposed process. The acquisition program office for Navy IT network systems is through the Program Executive Office (PEO) Command, Control, Communications, Computers, and Intelligence (C4I) Program Manager, Warfare (PMW) 160 Tactical Networks. The Programs of Record (POR's) under PMW 160 provide LAN and WAN connectivity to Navy tactical platforms and the proposed systems engineering process will be utilized and tailored to ensure that it can be used to assist in design and integration activities.

A. OVERVIEW OF NAVY IT TACTICAL SYSTEMS

Automated Digital Network System (ADNS) and Consolidated Afloat Networks and Enterprise Services (CANES) are the two current Programs of Record within PMW 160 that provide network transport and services on Navy Tactical Platforms. ADNS provides the WAN capability and CANES provides the LAN capability. Together, these programs encompass the network transport and work closely to ensure appropriate network transport on and off the platform to support the necessary information exchanges.

As the WAN provider, ADNS provides WAN routing services between platform and shore sites over limited bandwidth Satellite Communications (SATCOM), Line of Sight (LoS), and piers services. ADNS is the program that provides the network routing design for path selection. ADNS also provides WAN optimization services. This includes application compression to ensure that data is compressed for more effective usage of the limited bandwidth available. Network protocols are also enhanced using acceleration techniques to augment standard network protocols to work over limited bandwidth, high latency, and high error rate links. Lastly, ADNS provides load distribution of multiple

links when available to ensure all available resources are effectivity used and quality of service over those links to prioritize critical information exchanges over limited WAN connectivity (Program Executive Office; Command, Control, Communications, Computers, and Intelligence; Program Manager; Warfare 160 Tactical Networks [PEO C4I PMW 160] 2014).

As the LAN provider, CANES provides network infrastructure and services to the Navy tactical platforms and interfaces with the required shore-based applications to support the warfighters on the platforms. The CANES program provides server and workstation hardware and applications and a footprint for hosting of applications that are developed outside of PMW 160. These applications are termed "hosted" systems. CANES also provides network infrastructure for applications not managed by PMW 160 that bring their own hardware. These applications are termed "connected" systems. A CANES overview is provided in Figure 11. This depicts the applications and services that CANES provides. CANES consolidated a number of legacy programs into an overarching PoR for shipboard LAN's (PEO C4I PMW 160 2014).

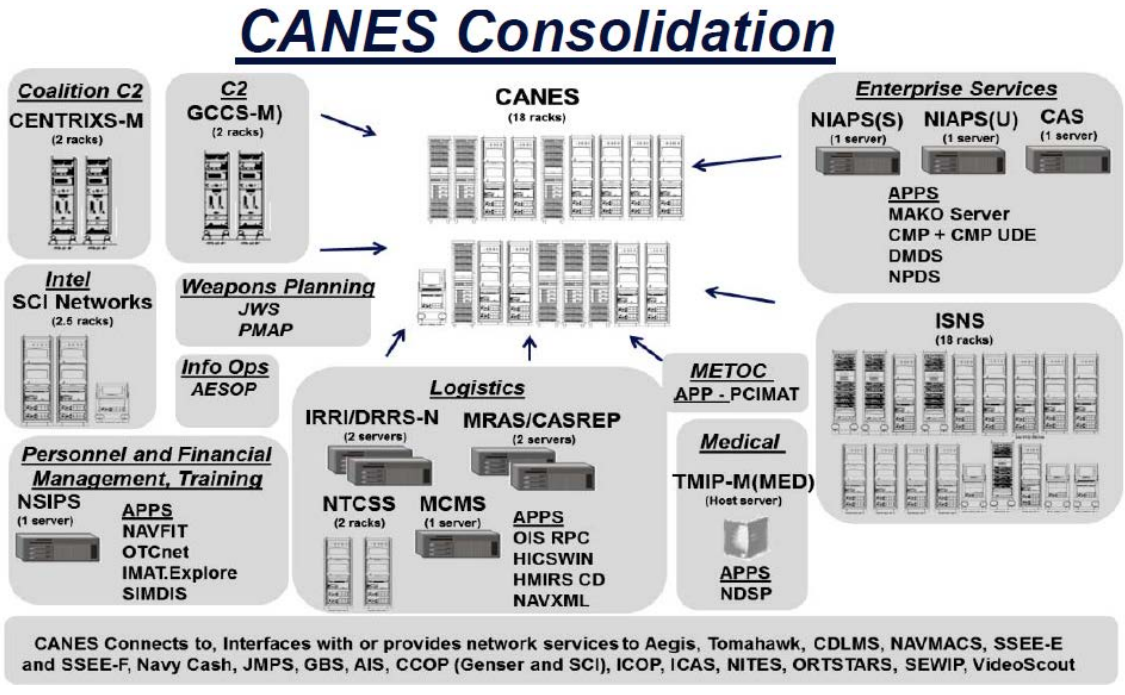

Figure 11. CANES Consolidation Overview. Source: PEO C4I PMW 160 (2014).

The specific components that make up CANES are provided in Figure 12. This includes workstations, application racks, network infrastructure, wireless access points, IP phones, and video teleconferencing (VTC) capability (PEO C4I PMW 160 2014).

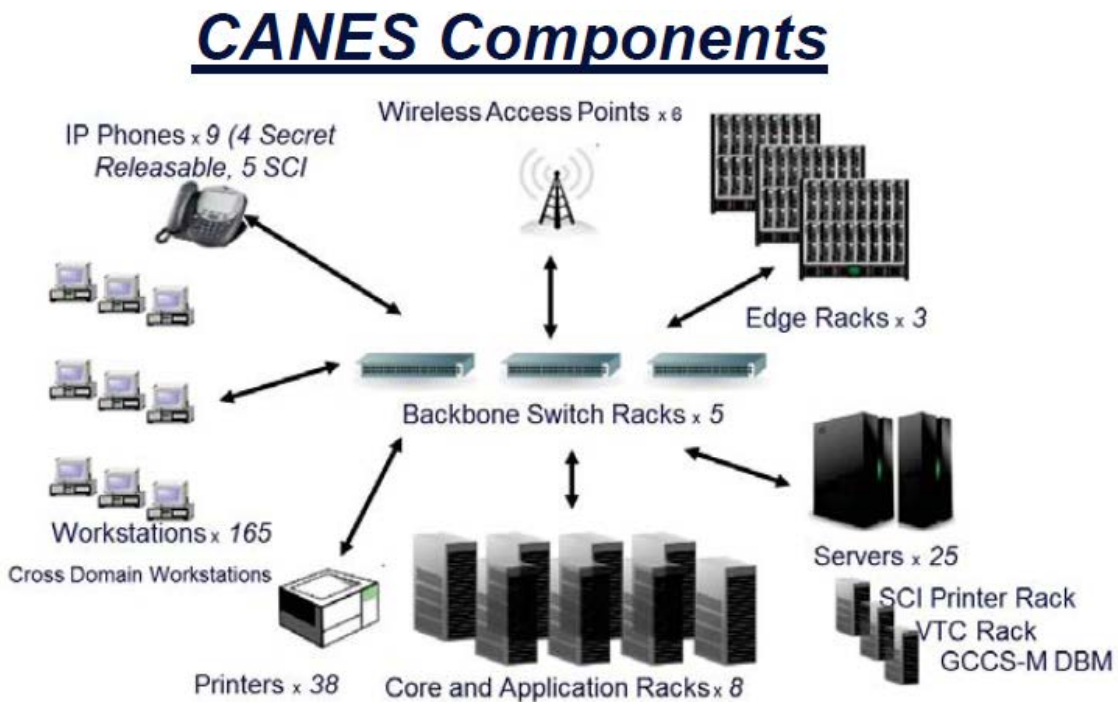

Figure 12. CANES Components. Source: PEO C4I PMW 160 (2014).

As CANES hosts and provides transport services to a variety of applications that are developed and sponsored outside of PMW 160, the sponsors of these applications work closely with PMW 160 to design, integrate, and install these applications on tactical platforms and capture the interfacing requirements to the networks via the Application Integration (AI) Process. This process was developed and maintained by the PMW 160 AI team and assessments and integration events are conducted on a recurring basis to allow applications to install on the LAN for Tactical Platforms (PEO C4I PMW 160 2014). The process and governance relationships are depicted in Figure 13.

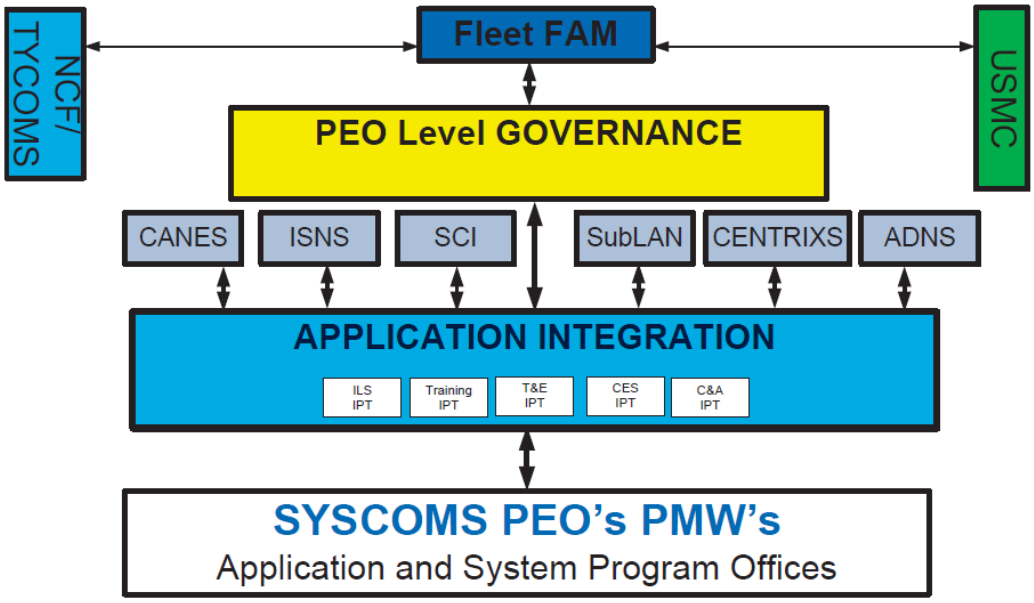

Figure 13. AI Process. Source: PEO C4I PMW 160 (2014).

B. CHALLENGES SPECIFIC TO NAVY IT TACTICAL SYSTEMS

Navy IT networks are a system of systems challenge for design and testing. This is due to a number of factors specific to the Navy tactical platform architectures. These unique challenges are detailed in this section from the general network transport case. A typical LAN and WAN diagram for the Navy environment that highlights some of the magnified challenges faced in this environment is provided in Figure 14.

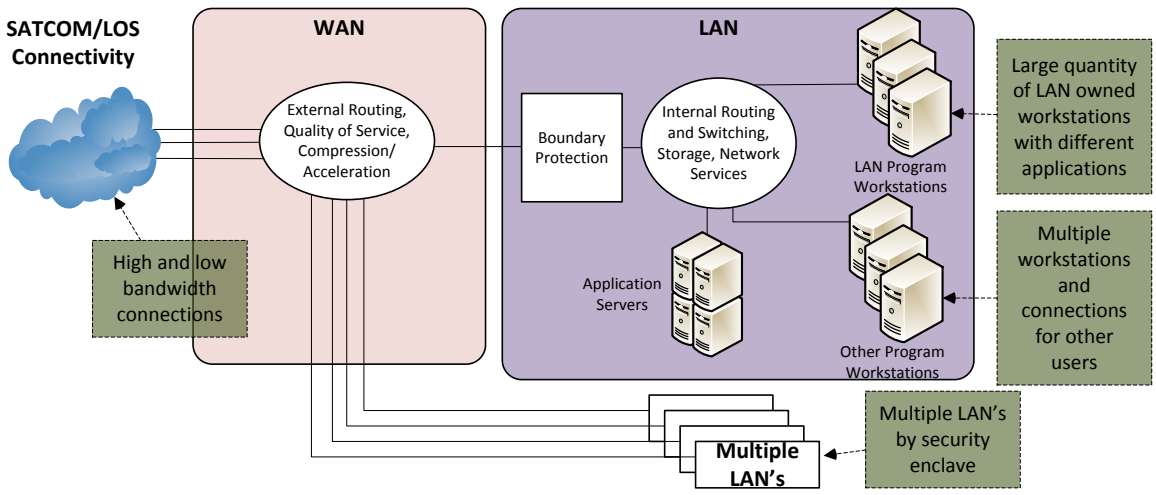

Figure 14. Challenges for a Navy Shipboard Platform.

Specific challenges that are more heightened on Navy shipboard platforms include a large diversity of programs of record that make up the IT systems, a large number of independent security enclaves that all utilize the same transport off the platform, and a dynamic mixture of SATCOM data rates and link types that can have large variances on the available capacity of WAN bandwidth. The platform will need to support critical applications within the possible ranges of bandwidth.

1. Diversity of Systems

There is a large diversity of programs of record that make up the IT systems (PEO C4I PMW 160 2014), to include multiple programs for SATCOM systems and line of sight tactical radios, a program for the WAN, a program for the LAN, and hundreds of hosted and connected applications that connect to the LAN, some of which are not formal programs of record or are in a different acquisition command. This diversity causes challenges in coordination and alignment in fielding. This leads to a disconnect in funding profiles, fielding schedules, and a lack of system of system requirements that can be identified and governed. Instead of being managed by a single IT department as typical in a business environment, a number of different programs need to integrate together with different program managers and supporting personnel for network transport

capability on tactical platforms. No single overarching governance therefore exists due to the number of program managers involved.

This diversity of programs and lack of alignment leads to a large number of baselines fielding across the platforms. This causes a challenge for common requirements, design, and integration. As discussed later in this section, an ability to assess network design performance in a number of different configurations and architectures is critical to address the number of baselines fielding.

2. Multiple Enclaves

Tactical platforms contain a number of security enclaves with different applications and users (PEO C4I PMW 160 2014). Each of the enclaves are encrypted and aggregated for transport off the platform. The limited bandwidth resources need to be divided up amongst each of the enclaves to ensure support of the various missions that the platform is conducting. Oftentimes, users in various locations are supporting different missions within each enclave. A detailed understanding of the data flows amongst each enclave is therefore critical to ensure that, across the enclaves, the appropriate missions are being supported. This should be fed into the collection of information exchange requirements to ensure the enclave is identified and utilized in the network bandwidth assessment to capture the requirements of transport for each enclave.

3. Bandwidth Variations and Combinations

Tactical platforms rely on SATCOM and line of sight communications for network transport when deployed and pierside terrestrial connections when connected to the pier. The SATCOM and LoS links can vary widely from low kbps of data rates to multiple Mbps and higher with the newer Wideband SATCOM connections (Program Manager, Warfare/Air [PMW/A] 170 2011). The WAN transport system, ADNS, also is designed to leverage bandwidth from all the available links when multiple links are available. The data rates from each individual link and combination of all links together give an overall available bandwidth for the platform (Department of the Navy 2015).

In conjunction with these bandwidth considerations, the data rates over these links are typically not sufficient for the applications on the networks and leads to an oversubscription of bandwidth. Additionally, data rate information by each application is typically not well known or accurate to understand the level of oversubscription that needs to be managed. Similar to the commercial environment, user interaction with software applications and changes to the application interfacing can cause changes to the data rates utilized over the network. Therefore, testing in a laboratory environment and measurements of data rates during that testing may not reflect what data rate is actually observed in an operational environment. Developers of applications may also not measure the data rate through the network, which yields no information on the data rate until it is integrated into a lab environment with the network.

Bandwidth oversubscription, in conjunction with limited knowledge of per-application data rate requirements, poses a design challenge for network transport to support the platforms. Design assessment models need to account for the data rate variations and combinations of links available in a number of different topologies. The application performance needs to be considered in each of these conditions to fully understand the behavior of the network transport system. The model needs to be flexible to be able to support assessing a number of topologies while also accounting for the dynamic nature of applications through each of the topologies.

C. TACTICAL NETWORKS PROCESS USE CASE

The process identified in the previous chapter will be applied to the Navy platform IT environment. The below sections go through each step of the process and employ a use case for a Navy platform. A guided missile destroyer, the DDG class, was used as the representative platform for the use case to ensure clearly defined missions and applications could be considered. The information generated is representative of what would be utilized for a tactical platform and intended to be a guide for a more detailed assessment using this process. To support an actual design effort for a DDG network, a more detailed assessment would need to be done with all applications and refined data to

support design decisions and analyses. This thesis utilizes a subset of applications and missions as part of the use case scope to exercise the proposed SoSE&I process.

1. Identify Capabilities

The first step of the process is to identify the capabilities of the platform and the priority of those capabilities. Within the Navy, these capabilities are typically considered the different missions of the platform. Specific to a DDG, key mission areas considered in the use case include ballistic missile defense (BMD), anti-air warfare (AAW), and anti-submarine warfare (ASW) (Department of the Navy 2015). A DDG performs other missions such as strike warfare and anti-surface warfare but these are outside the scope of this use case assessment. In addition to these mission areas, the ship contains systems to support logistics and personnel training (PEO C4I PMW 160 2014) that are outside of these specific mission areas but needed for operations of the ship. The prioritization of the capabilities is a critical component of designing and implementing an IT network and governance involvement is critical to ensure that the right capabilities are identified and in the appropriate prioritization order to complete the design. Instead of using a high/ medium/low approach from the previous section, a numerical prioritization value was utilized for the use case between one and four for each capability, with one being the highest priority. This scale can be tailored to accommodate a larger numerical range based on the number of capabilities of the SoS. A prioritization level is required to ensure proper assessment of the capabilities when not all can be supported at the same time. Due to the criticality of the mission and potential impact if a ballistic missile successfully strikes an area, ballistic missile defense (BMD) was considered the highest priority of the platform for the use case. Anti-air warfare (AAW) and anti-submarine warfare (ASW) were next at number two as they are critical to defense within the region and of the platform itself. These areas are still critical to the platform but the impact is less than with BMD if the capability cannot be supported. Logistics was selected at a number three. The information exchanges for logistics are typically less time sensitive but the data is still needed to get between the platform and shore sites to ensure equipment is being maintained and that any parts are ordered as needed. Lastly, morale, welfare, and recreation (MWR) for the sailors on the platform is priority number four. This includes

training and financial transactions. These activities are important to maintain morale for the sailors and support the daily shipboard operations but should not be prioritized over mission critical information exchanges when defense of a nation or the platform needs to be supported. The capabilities and priorities for the use case are provided in Table 6.

Table 6. Navy Use Case – Capability and Priority. Adapted from Department of the Navy (2016).

Capability/Mission	Priority	Description
BMD	1	Network traffic critical to BMD planning and execution
AAW	2	Network traffic critical to AAW planning and execution
ASW	2	Network traffic critical to ASW planning and execution
Logistics	3	Network traffic in support of the logistics that is not as time critical (parts replenishment, maintenance information)
MWR	4	Non-critical network traffic in support of sailor leisure (web browsing, personal email)

2. Identify Information Exchanges

Once the capabilities are identified and prioritized, the next step is to identify the information exchanges needed for each capability. For purposes of the use case, CANES systems were used to identify representative information exchanges for each capability. This is identified as a sample use case to depict the concept for purposes of this thesis and needs to be refined and expanded for an actual assessment. The sample set of information exchanges for this use case is listed in Table 7. This is based on an assumption that each capability requires a planning function, awareness of the battlefield through a common operational picture (COP), file transfers for the mission, and coordination via phone or VTC.

Table 7. Navy Use Case – Information Exchanges. Adapted from PEO C4I PMW 160 (2014).

Capability	Priority (1-4)	Information Exchanges	Description
BMD	1	Command and Control (C2)	C2 of sensors and tracking in support of BMD
		Common Operational Picture (COP)	Track exchange for BMD
		Mission Planning	Plan missions to support BMD
		File Transfers	Support transfer of files in support of mission
AAW	2	COP	Track exchange for AAW
		Mission Planning	Plan missions to support AAW
		File Transfers	Support transfer of files in support of mission
ASW	2	COP	Track exchange for ASW
		Mission Planning	Plan missions to support ASW
		File Transfers	Support transfer of files in support of mission
Logistics	3	Mission Critical Email	Communications with manufacturers and shore-based logistics personnel
		File Transfers	Distribution of manuals and other logistics information
		Mission Critical Web	Access to websites for logistics information
MWR	4	Non-Critical Email	Email for personal communications
		Non-Critical Web	Web access for personal usage

3. Map Applications to Information Exchanges

The next step is to map the applications to the information exchanges. This is important to be able to understand how the application is supporting the capabilities of the platform. This is typically not a focus of network design efforts due to the complexity and number of applications, but an up to date list of information exchanges and applications is critical to ensuring that the IT network is designed to support the platform capabilities.

One of the challenges apparent through the mapping process is that some applications span multiple information exchanges and capabilities. This makes it challenging to prioritize one application supporting a higher priority capability over a lower priority capability as the application supports multiple capabilities. If the information exchange uses the same ports and protocols, the quality of service algorithms will not be able to differentiate information exchanges between the capabilities. Therefore, data flows from that application cannot be prioritized between the capabilities and the network transport assessment will have to take that into account when assessing the network transport. Network redesign could be a consideration by either hosting multiple applications, one for each capability, or moving to unique ports or protocols. However, both of these increase the complexity and cost of implementation as well as increasing size, weight, and power (SWaP) if additional hardware is needed when splitting out the applications for differentiation.

A mapping of information exchanges to applications, as well as the enclave and minimum and maximum data rates, is provided in Table 8. The data rate numbers were estimated to depict the methodology for the use case based on expected data rates for each of the protocols used (Miller 2004) and applications selected are representative of shipboard applications, such as Command and Control Processor (C2P) and Global Command and Control System–Maritime (GCCS-M) (Department of the Navy 2015). Three main data rate values were selected for this assessment. For lower bandwidth applications such as COP, a minimum of 25 kbps and maximum of 50 kbps was utilized. For medium bandwidth applications such as file transfers, a minimum of 100 kbps and maximum of 300 kbps was utilized. For high bandwidth applications such as email and

web, a minimum of 500 kbps and maximum of 1 Mbps was utilized. These data rate numbers need to be refined in an actual assessment using measured data rate numbers as identified in the application design and testing efforts. The values used in this assessment are not representative of the actual application data rate requirements or measured values and intended to depict how an assessment would be done once the values are known.

Table 8. Navy Use Case – Information Exchanges to Applications. Adapted from Miller (2004) and Department of the Navy (2015).

Capability	Information Exchanges	Application	BW Usage	Min Data Rate (kbps)	Peak Data Rate (kbps)
BMD	Command and Control (C2)	C2P	Low	25	50
	COP	C2P	Low	25	50
		GCCS-M	Low	25	50
	Mission Planning	BMD Mission Planner	Med	100	300
	File Transfers	Workstations	Med	100	300
	Voice	VoIP Handsets	Med	100	300
AAW	COP	GCCS-M	Low	25	50
	Mission Planning	AAW Mission Planner	Med	100	300
	File Transfers	Workstation	Med	100	300
	Voice	VoIP Handsets	Med	100	300
ASW	COP	GCCS-M	Low	25	50
	Mission Planning	ASW Mission Planner	Med	100	300
	File Transfers	Workstations	Med	100	300
Logistics	Mission Critical Email	Email Server	High	500	1000
	File Transfers	Workstations	Med	100	300

Table 8 (continued)

	Mission Critical Web	**Web Proxy Server**	**High**	**500**	**1000**
	VTC	VTC System	Med	100	300
	Voice	VoIP Handsets	Med	100	300
MWR	Non-critical Email	Email Server	High	500	1000
	Non-Critical Web	Web Proxy Server	High	500	1000

4. Design and Performance Assessment

The design and performance assessment is a key component of the process. The information gathered on applications and information exchanges needs to be modeled to understand the behavior of the network to support the modification of the design to support the needed capabilities. As identified in the previous chapter, three key components feed into the design and performance assessment. These components are the data flow parameters, available bandwidth, and the scenarios. These are detailed in the remainder of this section.

a. Components of Design and Performance Assessment

The data flow parameters are taken from the previous step of mapping of applications to information exchanges. This information is utilized in the model or analysis for the design and performance assessment as an input to ensure that the data flows are properly characterized.

The available bandwidth is the next input. A depiction of satellite links available for a DDG and the typical data rates projected is in Table 9. The representative values for data rates for this use case were selected for a DDG based on typical bandwidth values available for the platform (Fisko 2011). A combination of military and commercial satellite communications is employed on Navy platforms. Within military SATCOM, the Navy Multiband Terminal (NMT) connects through the Wideband Global SATCOM

(WGS) constellation for Super High Frequency (SHF) connectivity and Extremely High Frequency (EHF) SATCOM through Advanced EHF (AEHF) satellites. Commercial SATCOM is available through the Commercial Broadband SATCOM Program (CBSP) (Fisko 2011).

Table 9. Navy Use Case – Link Types and Data Rates. Adapted from Fisko (2011).

Link Type	Data Rates
High Wideband MILSATCOM	8 Mbps
Low Wideband MILSATCOM	4 Mbps
COMSATCOM	2 Mbps
High EHF	256 Kbps
Low EHF	64 Kbps

The next step is to identify the specific scenarios to use for the assessment. A number of different iterations need to be looked at for each assessment based on the potential for varying data rates for a platform based on SATCOM connectivity and the environment of the operational platform. This is depicted in Table 10. Different regions have varying satellite resources available, translating to different expected data rates per link, so this needs to be tailored to reflect data rates expected.

The first scenario is a higher bandwidth scenario with higher MILSATCOM links, a COMSATCOM link, and a high EHF link available for WAN connectivity for an aggregate of 10.256 Mbps for the platform. The second scenario reduces the overall capacity of the MILSATCOM link, for an aggregate data rate of 6.256 Mbps for the platform. The third scenario reduces the capacity by removal all MILSATCOM connectivity. This leaves access to COMSATCOM and EHF SATCOM for an aggregate of 2.256 Mbps. The fourth scenario contains only higher EHF protected SATCOM data rates for an aggregated bandwidth of 256 kbps. The last scenario has only reduced EHF connectivity for an available bandwidth of 64 kbps. Assessing each of the scenarios is important as a platform can have a range of an aggregate bandwidth based on equipment

availability, location of the platform and corresponding access to satellite resources, and competition with other platforms for the limited satellite resources.

Table 10. Navy Use Case – Aggregate Bandwidths for Assessment. Adapted from Fisko (2011).

	High SHF MIL SATCOM 8 Mbps	Low SHF MIL SATCOM 4 Mbps	COM SATCOM 2 Mbps	High EHF 256 Kbps	Low EHF 64 Kbps	Total (Mbps)
Scenario 1	X		X	X		10.256
Scenario 2		X	X	X		6.256
Scenario 3			X	X		2.256
Scenario 4				X		0.256
Scenario 5					X	0.064

b. Priority Queuing Assessment

Once the data flow parameters, data rates, and scenarios are identified, the actual assessment needs to occur to determine the optimal QoS configuration to support the information exchange requirements and make tradeoffs in scenarios where the information exchanges cannot be supported. Governance is a key piece to ensure that the tradeoffs and limitations are clearly understood and agreed upon. Several approaches could be utilized to support this assessment and these approaches differ based on the QoS policy utilized for traffic prioritization. The simplest QoS policy to model and assess is priority queuing based on a straightforward mapping of capability prioritization to a queue priority. Priority queuing uses rules to differentiate different priority levels, typically based on a value on the IP packet called a Type of Service (ToS) field to classify the packet into the appropriate priority queue. This ToS field has different settable values that can be used to define different priority levels (Miller 2004). Priority

queueing will transmit all traffic of a higher priority queue before moving to the next priority level, sending all of the traffic from the second level, then moving on to the next priority level. Each of the priority queues utilizes a first in first out (FIFO) behavior that sends the oldest packets in the queue out first when the queue is being used for transmit. This continues until there is no more bandwidth available or no more traffic to send. One of the disadvantages of priority queuing is that it can result in "starvation" of the lower priority queues, where the higher priority queues consume all of the bandwidth (Park 2005). A depiction of priority queuing behavior is provided in Figure 15.

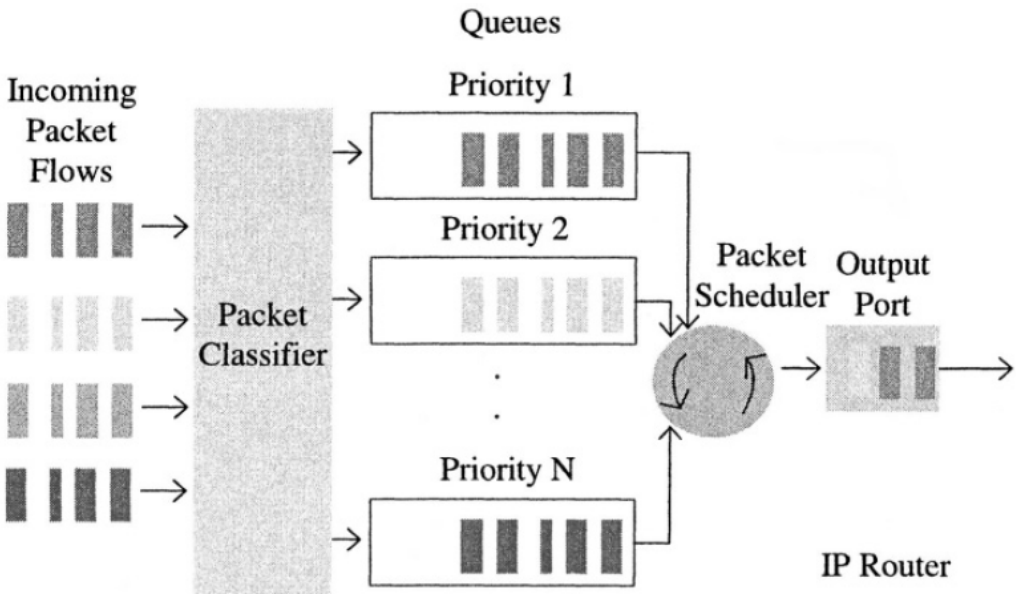

Figure 15. Priority Queuing. Source: Park (2005, 138).

Priority queuing has restricted use within tactical networks but will be utilized to support this assessment based on the predictability of the QoS behavior and simplicity of the assessment to be able to characterize data flow behavior over priority queuing. A summation of data flows can be utilized to determine the break point of the applications and corresponding capabilities that are supported by the applications for each of the scenarios. In this example, each capability has a different priority level, with the highest priority level being assigned to BMD.

An assessment under priority queuing with the various scenarios and data rates for this use case is depicted in Table 11. Microsoft Excel was utilized to populate the capabilities, applications, and data flow characteristics to conduct the assessment. Using the aggregated data rates from the scenarios and conducting a summation of the application data rates, a color-coded spreadsheet was created to depict the breaking point of applications over the WAN links for each of the capabilities. This allows a clear depiction of the overall bandwidth requirements, what scenarios the bandwidth is supported, and what capabilities are not able to be supported when restricted by limited throughput. This first assessment was completed using the minimum bandwidth values for each application. The colors depict the support for each capability, where green shows that the applications can be supported for each scenario and red shows that the bandwidth has been exceeded and, in a strict priority queuing model, the application is not supported due to congestion. Note that several of the applications, such as GCCS-M and the Voice over Secure IP applications, support multiple capabilities. These bandwidth values for these applications are summarized for the first capability where this application is needed. From a QoS perspective at the network devices, the application cannot be differentiated so it has to be considered for the QoS prioritization of the highest capability in the overall aggregation of bandwidth.

From looking at the table, the red colors for scenario 4 and 5, EHF only, depict that most of the capabilities cannot be supported in those scenarios. Scenario 3 is also degraded for logistics and cannot support MWR. This would indicate that additional investments should be considered for EHF data rates, the platform should increase the satellite allocation in those scenarios, or applications should be designed to support a reduced data rate to support those capabilities.

Table 11. Navy Use Case – Capability and Priority. Adapted from Miller (2004) and Department of Navy (2015).

Capability/ Mission	Application	Min Data Rate	Aggregate Min Demand (kbps)	Scenario 1 Min	Scenario 2 Min	Scenario 3 Min	Scenario 4 Min	Scenario 5 Min
BMD	C2P	25	25	10231	6231	2231	231	39
	C2P	25	50	10206	6206	2206	206	14
	GCCS-M	25	125	10131	6131	2131	131	-61
	BMD Mission Planner	100	225	10031	6031	2031	31	-161
	Workstations	100	325	9931	5931	1931	-69	-261
	VoSIP Handsets	100	425	9831	5831	1831	-169	-361
AAW	GCCS-M (common with BMD)	25	425	9831	5831	1831	-169	-361
	AAW Mission Planner	100	525	9731	5731	1731	-269	-461
	Workstation	100	625	9631	5631	1631	-369	-561
	VoSIP Handsets (common with BMD)	100	725	9531	5531	1531	-469	-661
ASW	GCCS-M (common with BMD)	25	725	9531	5531	1531	-469	-661
	ASW Mission Planner	100	825	9431	5431	1431	-569	-761
	Workstations	100	925	9331	5331	1331	-669	-861
Logistics	Email Server	500	1925	8331	4331	331	-1669	-1861
	Workstations	100	2025	8231	4231	231	-1769	-1961
	Web Proxy Server	500	2525	7731	3731	-269	-2269	-2461
	Tandberg VTC System	100	2625	7631	3631	-369	-2369	-2561
	VoIP Handsets	100	2725	7531	3531	-469	-2469	-2661
MWR	Email Server (common with logistics)	500	2725	7531	3531	-469	-2469	-2661
	Web Proxy Server	500	3225	7031	3031	-969	-2969	-3161

An assessment under strict priority queuing with the various scenarios and data rates using the maximum bandwidth values is depicted in Table 12. The colors again depict the support for each capability, where green shows that the applications can be supported for each scenario and red shows that the bandwidth has been exceeded under congestion. Since this assessment uses the application maximum bandwidth data rates, there is additional degradation in the capabilities. Scenario 2, lower MILSATCOM data rates, is not able to support MWR and is degraded for logistics, where scenario 3 with COMSATCOM and EHF indicates degradation with ASW.

Table 12. Navy Use Case – Priority Queuing Assessment. Adapted from Miller (2004) and Department of Navy (2015).

Capability/ Mission	Application	Peak Data Rate	Aggregate Max Demand (kbps)	Scenario 1 Max	Scenario 2 Max	Scenario 3 Max	Scenario 4 Max	Scenario 5 Max
BMD	C2P	50	50	10206	6206	2206	206	14
	C2P	50	100	10156	6156	2156	156	-36
	GCCS-M	50	250	10006	6006	2006	6	-186
	BMD Mission Planner	300	550	9706	5706	1706	-294	-486
	Workstations	300	850	9406	5406	1406	-594	-786
	VoSIP Handsets	300	1150	9106	5106	1106	-894	-1086
AAW	GCCS-M (common with BMD)	50	1150	9106	5106	1106	-894	-1086
	AAW Mission Planner	300	1450	8806	4806	806	-1194	-1386
	Workstation	300	1750	8506	4506	506	-1494	-1686
	VoSIP Handsets (common with BMD)	300	2050	8206	4206	206	-1794	-1986
ASW	GCCS-M (common with BMD)	50	2050	8206	4206	206	-1794	-1986
	ASW Mission Planner	300	2350	7906	3906	-94	-2094	-2286
	Workstations	300	2650	7606	3606	-394	-2394	-2586
Logistics	Email Server	1000	4650	5606	1606	-2394	-4394	-4586
	Workstations	300	4950	5306	1306	-2694	-4694	-4886
	Web Proxy Server	1000	5950	4306	306	-3694	-5694	-5886
	Tandberg VTC System	300	6250	4006	6	-3994	-5994	-6186
	VoIP Handsets	300	6550	3706	-294	-4294	-6294	-6486
MWR	Email Server (common with logistics)	1000	6550	3706	-294	-4294	-6294	-6486
	Web Proxy Server	1000	7550	2706	-1294	-5294	-7294	-7486

A depiction of the resulting bandwidth assessment for each of the capabilities in each of the scenarios is shown in Table 13. This uses Table 8 and assessment results from Tables 11 and 12 to tie the applications to the capabilities to provide a status by capability for each of the scenarios for applications using minimum and maximum bandwidth values. A zero to two point scale was used to depict the status for each of the capabilities. A value of two means that both minimum and maximum bandwidth is supported for each of the applications supporting the capability in both best and worst case scenarios. This is depicted in a green color. A yellow color with a numerical value of one signifies that the minimum bandwidth requirements are met for a capability but not the maximum bandwidth requirements. Red, tied to a value of zero, designates that both minimum and maximum bandwidth requirements are not met for a given capability. Excel was again utilized to assess each of the scenarios for bandwidth support.

Table 13. Navy Use Case – Scenario Bandwidth Assessment.

	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
BMD	2	2	2	0	0
AAW	2	2	2	0	0
ASW	2	2	1	0	0
Logistics	2	1	0	0	0
MWR	2	1	0	0	0

A result of this assessment is that, under the limited bandwidth conditions of scenario 4 and 5, the data flows for all of the capabilities cannot be fully supported in either minimum or maximum conditions. A way to address this in the design phase is to try to create a new queue of traffic that is prioritized over the others and fits within the available bandwidth in the scenario with a subset of applications and information exchanges. For the case of BMD, BMD C2 could be the highest priority traffic type, and could be prioritized over the other BMD information exchanges within the BMD capability. A depiction of the results of the assessment where BMD C2 traffic is prioritized over BMD COP, mission planning, and voice is provided in Table 14. As noted, BMD C2 would be supported even under the lower bandwidth conditions. This shows the important of understanding each of the data flows and characteristics in designing and implementing network transport. This assessment is required to be able to understand system performance and to be able to make informed tradeoff decisions as needed. Governance is critical in this step to ensure that the right tradeoffs are being considered as part of the design solution.

Table 14. Navy Use Case – Capability and Priority.

The BMD capability was split into two different queues/capabilities to allow support over limited bandwidth

	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
BMD - C2	2	2	2	2	2
BMD - COP, Voice and Mission Planning	2	2	2	0	0
AAW	2	2	2	0	0
ASW	2	2	1	0	0
Logistics	2	1	0	0	0
MWR	2	1	0	0	0

This assessment could be expanded by including more advanced traffic profiles. Some of the capabilities may not be concurrent and the supporting bandwidth of applications for those capabilities would therefore need to be removed from the assessment, so this would impact the bandwidth analysis. The actual traffic profile of the application themselves will vary based on user behavior. This could be modeled with a probability distribution with results based on a confidence interval and requires an end to end understanding of the network. This is outside the scope of this thesis but would allow better characterization of the data flows and provide enhanced results of application behavior.

c. Complex Queuing Assessments

A more complex assessment is required for QoS prioritizations that are not FIFO or priority queuing-based. These QoS capabilities are used to allow a more distributed utilization of bandwidth where all traffic classes get a portion of bandwidth and the higher priority traffic flows can get an increased portion of the bandwidth (Park 2005). This would allow multiple capabilities to share limited bandwidth resources. These

capabilities would operate in a degraded environment at the expense of having the primary capability fully supported. The transport protocol, either TCP or UDP, would be important when more complex QoS assessments are being conducted. Applications using TCP will back off transmit rates under congestion and this would need to be modeled and assessed. This is beyond the scope of this thesis, but a number of modeling and simulation tools can be utilized to effectively emulate queuing behaviors. An understanding of the scenarios and data flows is critical to ensure that the output of the tools is applicable. One of the advanced queuing techniques includes Weighted Round Robin (WRR), in which different flows of traffic are grouped into individual classes. These classes of flows can each be allocated varying amounts of the overall bandwidth. Within each of the classes and their corresponding bandwidth allocation, flows are queued within a second layer of round robin queuing to differentiate the flows within each of the classes (Park 2005). This multiple layer queuing approach is more complex to model and assess within a range of scenarios and therefore would add to the complexity of the analysis. A diagram of the WRR is depicted in Figure 16. This behavior requires more detailed analysis tools and calculations to predict behavior during the design phase of the network transport.

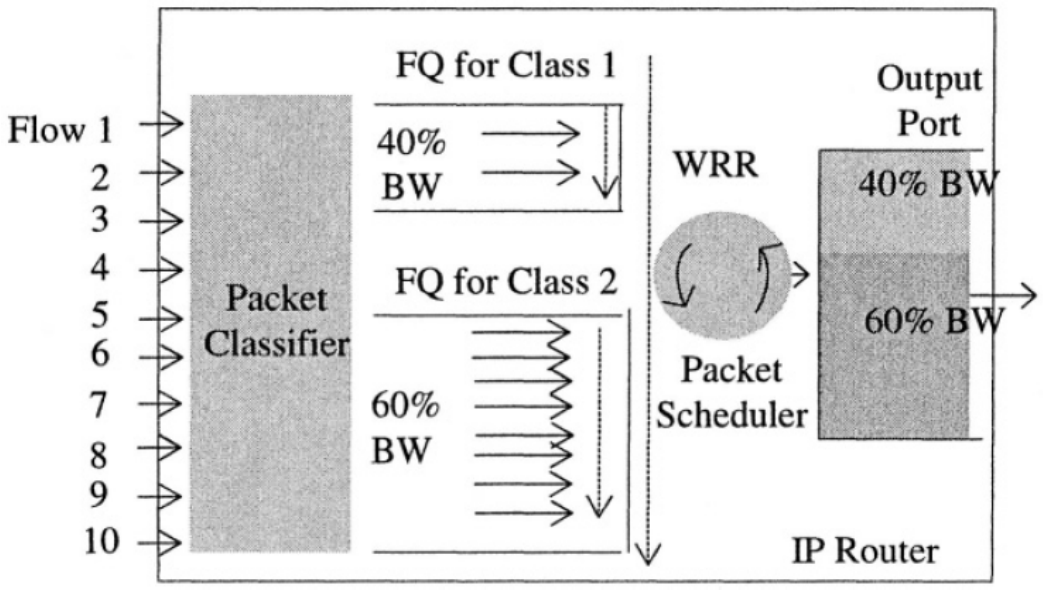

Figure 16. Weighted Round Robin. Source: Park (2005, 145).

5. Integration

There are several system of systems testing efforts currently used within PEO C4I to verify system interoperability prior to fielding as part of the overall SoSE&I efforts. The purpose of the Enterprise, Engineering, and Certification (E2C) testing is to identify, integrate, and verify key PEO C4I system interfaces prior to deployment, with a focus on surface platform and shore integration (Roa 2010). Common Submarine Radio Room (CSRR) system of systems testing is a test strategy that focuses on submarine C4I testing for the "acknowledged" SoS architectures within the submarine radio room. Unlike the Navy Surface C4I infrastructure, a formal PoR exists for integration of multiple systems within the submarine radio room. CSRR is the PoR responsible for this SoS architecture (NDIA, 2014). Application Integration (AI) is focused on integrating hosted and connected applications into the shipboard Local Area Network (LAN) and Wide Area Network (WAN) to ensure proper interoperability and configurations on the application, LAN, and WAN to support integration. The E2C, CSRR, and AI testing efforts focus on "platform-level" SoS integration for the surface and sub-surface platforms (Roa 2010).

Within these test environments, it is difficult to replicate the operational environment for the networks to validate proper design and integration. Specifically, many users and applications utilize the shipboard network infrastructure with potentially thousands of users present on larger Navy surface platforms. It is not cost effective or timely to replicate the amount of users and application set in a variety of different mission areas during testing. Secondly, minimal formal SoS requirements are currently available to test for proper integration within the C4I Programs. This can cause challenges in developing appropriate test cases and procedures without the SoS requirements clearly defined. Lastly, the number of different baselines on network transport, to include LAN, WAN, and applications, makes it difficult to emulate all of the variations in a test environment.

During the integration phase, the identified information exchanges and applications should be connected into the network and bandwidth should be monitored. This should be compared to the original values identified to ensure consistency. A representation of critical monitoring points is provided in Figure 17. Monitoring at the

LAN interface provides the application network load that is trying to be sent for data exchanges. Measuring at the WAN interface will provide the actual data rates provided to the applications based on WAN throughput and QoS implementation with prioritization of the traffic types.

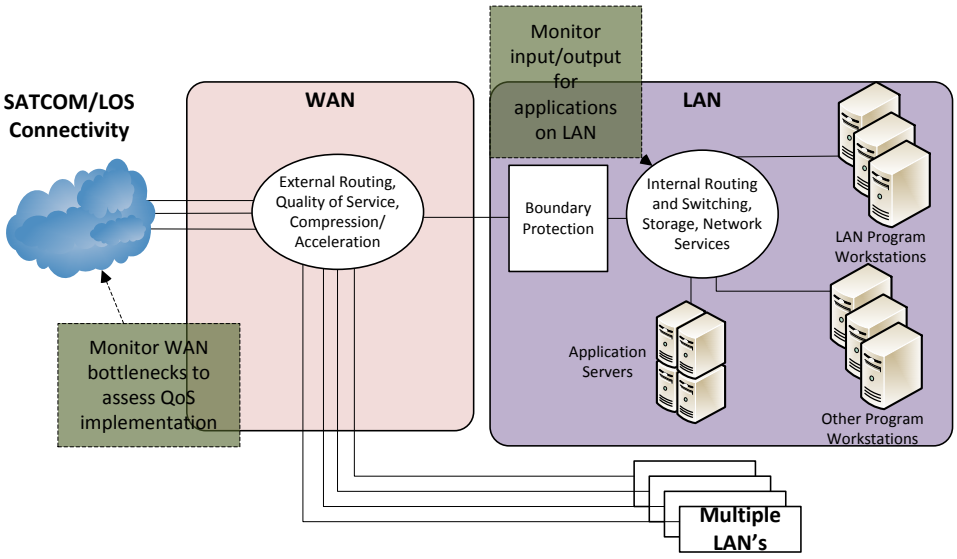

Figure 17. Monitoring Points for Bandwidth Assessment.

If any discrepancies are identified, the information should be updated. A depiction of the values that should be updated based on test and integration for each of the applications is provided in Table 15. This should then be fed back into the prior bandwidth assessment to ensure that any modifications do not change support of capabilities in the different scenarios. If they do, a design assessment will need to be conducted to determine the optimal design.

Table 15. Navy Use Case – Data Rate Updates.

Capability/ Mission	Information Exchange	Application	Min Data Rate	Peak Data Rate
BMD	Command and Control (C2)	C2P	25	50
	COP	C2P	25	50
		GCCS-M	25	50
	Mission Planning	BMD Mission Planner	100	300
	File Transfers	Workstations	100	300
	Voice	VoSIP Handsets	100	300
AAW	COP	GCCS-M (common with BMD)	25	50
	Mission Planning	AAW Mission Planner	100	300
	File Transfers	Workstation	100	300
	Voice	VoSIP Handsets (common with BMD)	100	300
ASW	COP	GCCS-M (common with BMD)	25	50
	Mission Planning	ASW Mission Planner	100	300
	File Transfers	Workstations	100	300
Logistics	Mission Critical Email	Email Server	500	1000
	File Transfers	Workstations	100	300
	Mission Critical Web	Web Proxy Server	500	1000
	VTC	Tandberg VTC System	100	300
	Voice	VoIP Handsets	100	300
MWR	Non-critical Email	Email Server (common with logistics)	500	1000
	Non-Critical Web	Web Proxy Server	500	1000

Update data rate values base on testing and integration

6. Monitoring

Upon implementation of the network on the platform, continued monitoring should occur for the SoS (Dahmann et al. 2010). Similar to the updates based on testing and integration, users and sites in an operational environment may utilize the applications differently than expected or change behaviors over time. This means that monitoring is required to ensure that the data rates expected are observed. If the data rates change, the information should be updated and a follow-on assessment should be conducted to ensure that the network is performing as intended. Based on the follow-on assessments, the network design may need to be updated and installed with the updates. Continued monitoring is needed to ensure that the updates to the system are behaving as expected as well. This monitoring would need to be done by operational users or during specific test events to ensure that the behavior is identified and any issues are considered for future design updates.

7. Governance

Governance should be a continual part of the process. However, there are key areas where governance needs to be considered to ensure that the appropriate decisions are being made (Vaneman and Jaskot 2013). The initial prioritizations of the capabilities require input from the governance body to ensure that the appropriate prioritization choices are being made (Vaneman and Jaskot 2013). Additionally, governance is needed at the end of the design and performance assessment. This will ensure that the selected and tested design supports the capabilities in a prioritization vetted through the governance. Any limitations to the design will need to be considered to ensure the design is suitable for implementation. Decisions on implementation of the QoS policy and what capabilities are supported in each scenario require input from the governance body to address any limitations identified and support any tradeoffs.

D. RESULTS OF USE CASE

This section provided an overview of how the network IT SoSE&I process could be applied to a Navy tactical platform use case. A sample use case for a DDG was utilized to go through each of the process steps to support a network bandwidth assessment. The results were used to look at trade off analyses that are possible with a simulation of data. Lastly, the importance of monitoring for any updates and governance was discussed at various points within the process to ensure that the information and resulting assessments are valid. A recommendation for QoS implementation identified in this section is to prioritize by capability or mission. This ensures that data flows and applications supporting those data flows can be grouped together and prioritized accordingly. Under congestion, the higher priority capabilities can utilize the bandwidth that is available over lower priority capabilities. Also, development of applications could focus on ensuring that data flows for different types of capabilities have unique characteristics that allow differentiation through the network transport. This allows unique identification to allow prioritization of data flows supporting one mission over another, even when a common application is utilized.

This assessment is intended to be a framework that can be leveraged. The actual assessment for a tactical platform will be more extensive with all enclaves and applications, to include refining application data rates with actual measured values. Additionally, the monitoring piece will be more extensive with frequent updates to the model required based on measured data during testing and deployment.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This thesis provided a model to conduct a network transport assessment using a repeatable, iterative process by tailoring previous SoS research to an IT network environment. This research and resulting process will help enhance IT network design and analysis by ensuring accurate information is available to characterize the systems within the SoS architecture during design activities, enhance end to end testing with more accurate and measured data, and support validation of engineering models to predict behavior. This research also can be used to support an early assessment of data exchange requirements for SoS systems to support trade off analyses earlier in the design phase for gap identification. A general IT network design was discussed in regards to the process. A more specific use case for Navy tactical platforms was then assessed using the proposed process. This allowed for verification of the steps and a use case to work through the various steps of the process.

A. RESULTS AND RECOMMENDATIONS

The findings of the research, development of the recommended process, and application to a use case addressed many of the primary research questions that were identified. The objectives of the thesis were met with the identified network IT SoSE&I process and use case. The benefits of the research will be to assist development, integration, and fielding of network IT systems with a tailored SoSE&I process. The individual research questions are listed below, with corresponding findings identified for each based on the research.

1. What are good systems, or SoS, engineering processes to utilize to address network transport design and testing?

This research question was addressed by defining a network IT SoSE&I process that was then applied to a use case. The process identified is recommended for usage by network IT designers and implementers when designing and implementing network IT systems and based on SoSE&I research and challenges specific to an IT environment.

When followed, it allows an iterative approach to identify and design to an environment that is rapidly changing.

2. How can SoS data throughput requirements be identified and assessed to support SoS design and testing activities?

During the use case, application throughput requirements were captured and assessed for a limited assessment. This can be extended to allow more granular assessments of the individual applications using the same framework and additional parameters of each of the applications. The research and use concluded that the correlation of application to capability is important to be able to assess application performance and implement these QoS policies that prioritize capabilities under congestion. Lastly, the prioritization of capabilities and the implementation of capability based QoS is important to ensure that network design and governance decisions can be made.

3. What characteristics of supporting tools and simulations are needed to model and characterize network performance as part of the identified systems engineering process?

As part of the use case, an excel model was utilized to capture application characteristics and assessing bandwidth capacity in a number of different scenarios. The core characteristics were identified but this research should be expanded to assess more complex QoS configurations and application behaviors. The importance of continuous monitoring of IT networks and the need to update the design to support new applications and changes to user behavior was identified as a finding of the research. This is critical due to the dynamic nature of networks.

4. Where should governance be applied to ensure the appropriate decisions are made in terms of identifying the appropriate data rates and QoS policies for the network?

The network IT SoSE&I process includes governance throughout the process to ensure that the appropriate design and development activities. Even though governance is needed throughout, governance is especially critical during the capability prioritization and after test and integration to ensure oversight of design and tradeoff decisions for network throughput.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

A limited assessment was done using a representative use case for Navy tactical platforms. The results of this should be used to conduct a more detailed analysis to include all applications and enclaves, identify a set of validated capabilities that are applicable to Navy platforms, and inclusion of the governance structure specific to the Navy environment to validate the design and integration. The third research question relating to defining characteristics of supporting tools and simulations was only lightly considered as part this assessment and should be further assessed with follow on efforts. A more detailed assessment of various tools to provide enhanced simulations of network loading will ensure an understanding of performance in a variety of network conditions. This will ensure appropriate network design activities and tradeoff decisions when designing, testing, and implementing network IT systems. Specific tools for monitoring of the network could also be considered for a follow on effort. These follow on efforts would allow an assessment of more complex QoS policies and application behaviors to ensure that the behavior of the network and applications is represented and understood to a larger degree of confidence.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Dahmann, Judith, George Rebovich, Ralph Lowry, JoAnn Lane, and Kristen Baldwin. 2011. "An Implementers' View of Systems Engineering for Systems of Systems." Accessed August 5, 2016. http://www.acq.osd.mil/se/docs/ImplementerViewSE-SOS-Final.pdf.

Dahmann, Judith, Jo Ann Lane, George Rebovich, and Ralph Lowry. 2010. "Systems of Systems Test and Evaluation Challenges." Accessed August 5, 2016. http://www.acq.osd.mil/se/docs/Dahmann-IEEE-SoSE%202010.pdf.

Department of the Navy. 2015. "U.S. Navy Program Guide 2015." Accessed August 5, 2016. http://www.navy.mil/strategic/top-npg15.pdf.

———. 2016. "United States Navy – Fact File Destroyers." January 13. http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=900&ct=413.

Fisko, Kurt. 2011. "Program Manager, Warfare/Air (PMW/A) 170 Communications Navy SATCOM Overview." October 26. http://www.afcea-la.org/filebrowser/download/619.

Miller, Mark. 2004. *internet Technologies Handbook: Optimizing the IP Network.* Hoboken, N.J.: John Wiley & Sons. Ebrary Reader e-book. http://www.ebrary.com/corp/.

National Defense Industrial Association (NDIA). 2014. "NDIA San Diego 2014 Fall C4I Industry Days." October 29. http://www.public.navy.mil/spawar/Press/Documents/Presentations/10.29.2014_NDIA-IndustryDay-2.pdf.

Office of the Deputy Under Secretary of Defense (ODUSD) for Acquisition and Technology (A&T), Systems and Software Engineering (SSE). 2008. *Systems Engineering Guide for Systems of Systems*. Washington, DC: ODUSD(A&T)SSE, August.

Park, Kun. 2005. *QoS in Packet Networks.* New York, New York: Springer Science & Business Media. Springer Link e-book. http://link.springer.com/.

PEO C4I PMW 160 (Program Executive Office; Command, Control, Communications, Computers, and Intelligence; Program Manager; Warfare 160 Tactical Networks). 2014. "CANES Overview." February 5. http://www.public.navy.mil/spawar/PEOC4I/ProductsServices/Documents/CANES_Overview_May14S.pdf.

Roa, Steve. 2010. "Team SPAWAR Enterprise, Engineering, and Certification (E2C) Initiative." August 10. http://www.ndia-sd.org/attachments/article/42/E2C.pdf.

Vaneman, Warren. 2016. “The System of Systems Engineering and Integration ‘Vee’ Model.” *Systems Conference (SysCon)*, 2016 IEEE International, 1–7.

Vaneman, Warren, and Roger Jaskot. 2013. “A Criteria-Based Framework for Establishing System of Systems Governance.” *Systems Conference (SysCon)*, 2013 IEEE International, 491–496. doi:10.1109/SysCon.2013.654992.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California